TigerSwitch 10/100/1000

Gigabit Ethernet Switch

- 12 auto-MDI/MDI-X 10/100/1000BASE-T ports
- 4 ports shared with 4 SFP transceiver slots
- Non-blocking switching architecture
- Support for a redundant power unit
- Spanning Tree Protocol
- Up to six LACP or static 4-port trunks
- Layer 2/3/4 CoS support through four priority queues
- Full support for VLANs with GVRP
- IGMP multicast filtering and snooping
- Support for jumbo frames up to 9 KB
- Manageable via console, Web, SNMP/RMON

SMC® Networks

Management Guide

SMC8612T

TigerSwitch 10/100/1000 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC® Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

July 2003
Pub. # 150200034800A

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2003 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618
All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:
http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE

FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

CONTENTS

1
Switch Management 1-1

Connecting to the Switch 1-1
Configuration Options 1-1
Required Connections 1-3
Remote Connections 1-4
Basic Configuration 1-5
Console Connection 1-5
Setting Passwords 1-6
Setting an IP Address 1-7
Enabling SNMP Management Access 1-10
Saving Configuration Settings 1-12
Managing System Files 1-13
System Defaults 1-14

2
Configuring the Switch 2-1

Using the Web Interface 2-1
Navigating the Web Browser Interface 2-2
Home Page 2-3
Configuration Options 2-3
Panel Display 2-4
Main Menu 2-5
Basic Configuration 2-8
Displaying System Information 2-8
Setting the IP Address 2-11
Security 2-14
Configuring the Logon Password 2-14
Configuring RADIUS/TACACS+ Logon Authentication . 2-16
Configuring HTTPS 2-21
Replacing the Default Secure-site Certificate 2-23
Configuring SSH 2-24
Managing Firmware 2-26
Downloading System Software from a Server 2-26
Saving or Restoring Configuration Settings 2-28

Copying the Running Configuration to a File 2-30
Displaying Bridge Extension Capabilities 2-31
Displaying Switch Hardware/Software Versions 2-34
Port Configuration 2-36
Displaying Connection Status 2-36
Configuring Interface Connections 2-38
Setting Broadcast Storm Thresholds 2-41
Configuring Port Mirroring 2-42
Configuring Port Security 2-44
Address Table Settings 2-47
Setting Static Addresses 2-47
Displaying the Address Table 2-49
Changing the Aging Time 2-51
Spanning Tree Protocol Configuration 2-51
STP Information 2-53
STP Configuration 2-57
STP Port and Trunk Information 2-61
STP Port and Trunk Configuration 2-65
VLAN Configuration 2-70
Assigning Ports to VLANs 2-71
Forwarding Tagged/Untagged Frames 2-73
Displaying Basic VLAN Information 2-74
Displaying Current VLANs 2-75
Creating VLANs 2-77
Adding Interfaces Based on Membership Type 2-79
Adding Interfaces Based on Static Membership 2-82
Configuring VLAN Behavior for Interfaces 2-83
Class of Service Configuration 2-87
Setting the Default Priority for Interfaces 2-87
Mapping CoS Values to Egress Queues 2-89
Setting the Service Weight for Traffic Classes 2-92
Mapping Layer 3/4 Priorities to CoS Values 2-93
Selecting IP Precedence/DSCP Priority 2-94
Mapping IP Precedence 2-94
Mapping DSCP Priority 2-97
Port Trunk Configuration 2-100
Dynamically Configuring a Trunk with LACP 2-102

Statically Configuring a Trunk 2-104
Configuring SNMP 2-106
Setting Community Access Strings 2-107
Specifying Trap Managers 2-109
SNMP IP Filtering 2-110
Multicast Configuration 2-113
Configuring IGMP Parameters 2-113
Interfaces Attached to a Multicast Router 2-117
Displaying Port Members of Multicast Services 2-119
Adding Multicast Addresses to VLANs 2-121
Showing Device Statistics 2-122
801.1X Port Authentication 2-129
802.1x Port Configuration 2-131
802.1x Statistics 2-134
Statistical Values 2-134

3
Command Line Interface 3-1

Using the Command Line Interface 3-1
Accessing the CLI 3-1
Console Connection 3-1
Telnet Connection 3-2
Entering Commands 3-4
Keywords and Arguments 3-4
Minimum Abbreviation 3-4
Command Completion 3-5
Getting Help on Commands 3-5
Partial Keyword Lookup 3-6
Negating the Effect of Commands 3-7
Using Command History 3-7
Understanding Command Modes 3-7
Exec Commands 3-8
Configuration Commands 3-9
Command Line Processing 3-10
Command Groups 3-12
General Commands 3-14
enable 3-14

disable 3-15
configure 3-16
show history 3-17
reload 3-18
end 3-18
exit 3-19
quit 3-19
Flash/File Commands 3-20
copy 3-21
delete 3-23
dir 3-24
whichboot 3-25
boot system 3-26
System Management Commands 3-27
hostname 3-29
username 3-30
enable password 3-31
jumbo frame 3-32
ip http port 3-33
ip http server 3-34
ip http secure-server 3-35
ip http secure-port 3-36
ip ssh 3-37
ip ssh server 3-38
disconnect ssh 3-39
show ssh 3-40
show ip ssh 3-40
logging on 3-41
logging history 3-42
logging host 3-44
logging facility 3-45
logging trap 3-45
clear logging 3-47
show logging 3-47
show startup-config 3-48
show running-config 3-51
show system 3-52

show users 3-53
show version 3-54
Authentication Commands 3-55
authentication login 3-56
radius-server host 3-58
radius-server port 3-58
radius-server key 3-59
radius-server retransmit 3-60
radius-server timeout 3-60
show radius-server 3-61
tacacs-server host 3-61
tacacs-server port 3-62
tacacs-server key 3-63
show tacacs-server 3-63
SNMP Commands 3-64
snmp-server community 3-65
snmp-server contact 3-66
snmp-server location 3-66
snmp-server host 3-67
snmp-server enable traps 3-69
snmp ip filter 3-70
show snmp 3-71
IP Commands 3-73
ip address 3-74
ip dhcp restart 3-75
ip default-gateway 3-76
show ip interface 3-77
show ip redirects 3-78
ping 3-78
Line Commands 3-80
line 3-81
login 3-82
password 3-83
exec-timeout 3-84
password-thresh 3-85
silent-time 3-86
databits 3-87

parity 3-88
speed 3-89
stopbits 3-90
show line 3-90
Interface Commands 3-91
interface 3-92
description 3-93
speed-duplex 3-94
negotiation 3-95
capabilities 3-96
flowcontrol 3-97
shutdown 3-99
switchport broadcast 3-100
port security 3-101
clear counters 3-102
show interfaces status 3-103
show interfaces counters 3-104
show interfaces switchport 3-106
Address Table Commands 3-107
mac-address-table static 3-108
show mac-address-table 3-109
clear mac-address-table dynamic 3-111
mac-address-table aging-time 3-111
show mac-address-table aging-time 3-112
Spanning Tree Commands 3-113
spanning-tree 3-114
spanning-tree mode 3-115
spanning-tree forward-time 3-116
spanning-tree hello-time 3-117
spanning-tree max-age 3-118
spanning-tree priority 3-119
spanning-tree pathcost method 3-120
spanning-tree transmission-limit 3-121
spanning-tree cost 3-122
spanning-tree port-priority 3-123
spanning-tree portfast 3-124
spanning-tree edge-port 3-125

spanning-tree protocol-migration 3-126
spanning-tree link-type 3-127
show spanning-tree 3-128
VLAN Commands 3-130
vlan database 3-131
vlan 3-132
interface vlan 3-133
switchport mode 3-134
switchport acceptable-frame-types 3-135
switchport ingress-filtering 3-136
switchport native vlan 3-137
switchport allowed vlan 3-138
switchport forbidden vlan 3-139
show vlan 3-140
GVRP and Bridge Extension Commands 3-141
switchport gvrp 3-142
show gvrp configuration 3-143
garp timer 3-144
show garp timer 3-145
bridge-ext gvrp 3-146
show bridge-ext 3-147
IGMP Snooping Commands 3-148
ip igmp snooping 3-149
ip igmp snooping vlan static 3-150
ip igmp snooping version 3-151
show ip igmp snooping 3-152
show mac-address-table multicast 3-152
ip igmp snooping querier 3-153
ip igmp snooping query-count 3-154
ip igmp snooping query-interval 3-155
ip igmp snooping query-max-response-time 3-156
ip igmp snooping router-port-expire-time 3-157
ip igmp snooping vlan mrouter 3-158
show ip igmp snooping mrouter 3-159
Priority Commands 3-160
switchport priority default 3-161
queue bandwidth 3-162

queue cos-map 3-163
show queue bandwidth 3-165
show queue cos-map 3-166
map ip precedence (Global Configuration) 3-166
map ip precedence (Interface Configuration) 3-167
map ip dscp (Global Configuration) 3-169
map ip dscp (Interface Configuration) 3-170
show map ip precedence 3-171
show map ip dscp 3-172
Mirror Port Commands 3-174
port monitor 3-174
show port monitor 3-175
Port Trunking Commands 3-177
channel-group 3-178
lacp 3-179

A
Troubleshooting A-1
Troubleshooting Chart A-1

B
Upgrading Firmware via the Serial Port B-1

Glossary

Index

CHAPTER 1
SWITCH MANAGEMENT

Connecting to the Switch

Configuration Options

The TigerSwitch 10/100/1000 includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is assigned via DHCP by default. To change this address, see "Setting an IP Address" on page 1-7.

The switch's HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics graphically using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch's Web management interface can be accessed from any computer attached to the network.

The switch's management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using management software.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's CLI configuration program, Web interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download of system firmware via TFTP
- Upload and download of switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to six static or LACP trunks
- Enable jumbo frame support
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in Appendix C.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.

2. Connect the other end of the cable to the RS-232 serial port on the switch.

3. Make sure the terminal emulation software is set as follows:
    - Select the appropriate serial port (COM port 1 or COM port 2).
    - Set the data rate to 9600 baud.
    - Set the data format to 8 data bits, 1 stop bit, and no parity.
    - Set flow control to none.
    - Set the emulation mode to VT100.
    - When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

4. Once you have set up the terminal correctly, the console login screen will be displayed.

Note: Refer to "Line Commands" on page 3-80 for a complete description of console configuration options.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 3-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 3-12.

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is assigned via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 1-7.

Note: This switch supports four concurrent Telnet sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a Web

browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.

2. At the Username prompt, enter "admin."

3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.)

4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the "username" command, record them and put them in a safe place.

Passwords can consist of up to eight alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level.

2. Type "configure" and press <Enter>.

3. Type "username guest password 0 *password*," for the Normal Exec level, where *password* is your new password. Press <Enter>.

4. Type "username admin password 0 *password*," for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:
CLI session with the SMC8624T is opened.
To end the CLI session, enter [Exit].
Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is assigned via DHCP by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address *ip-address netmask*," where "ip-address" is the switch IP address and "netmask" is the network mask for the network. Press <Enter>.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway *gateway*," where "gateway" is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the "bootp" or "dhcp" option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the "ip dhcp restart" command to start

broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the “bootp” or “dhcp” option is saved to the startup-config file, then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. At the interface-configuration mode prompt, use one of the following commands:

    - To obtain IP settings through DHCP, type “ip address dhcp” and press <Enter>.

    - To obtain IP settings through BOOTP, type “ip address bootp” and press <Enter>.

3. Type “exit” to return to the global configuration mode. Press <Enter>.

4. Type “ip dhcp restart” to begin broadcasting service requests. Press <Enter>.

5. Wait a few minutes, and then check the IP configuration settings, by typing the “show ip interface” command. Press <Enter>.

6. Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, it is recommended that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server community *string mode*," where "string" is the community access string and "mode" is **rw** (read/write) or **ro** (read only). Press <Enter>.
2. To remove an existing string, simply type "no snmp-server community *string*," where "string" is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community mis rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server host *host-address community-string*," where "host-address" is the IP address for the trap receiver and "community-string" is the string associated with that host. Press <Enter>.

2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type "snmp-server enable traps *type*," where "type" is either **authentication** or **link-up-down**. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in non-volatile storage, you must copy the running configuration file to the start-up configuration file using the "copy" command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, Web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — These files store system configuration information and are created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See "Saving or Restoring Configuration Settings" on page 2-28 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI, Web and SNMP management interfaces. See "Managing Firmware" on page 2-26 for more information.

- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test). This code also provides a facility to upload firmware files to the system directly through the console port. See "Upgrading Firmware via the Serial Port" on page B-1.

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file namethat reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file. See "Saving or Restoring Configuration Settings" on page 2-28.

The following table lists some of the basic system defaults.

Function	Parameter	Default
IP Settings	Management VLAN	1
	DHCP	Enabled
	BOOTP	Disabled
	User Specified	Disabled
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0

Function	Parameter	Default
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
SNMP	Community Strings	“public” (read only) “private” (read/write)
	Authentication Failure Traps	Enabled
	Link-up-Down Traps	Enabled
Security	Privileged Exec Level	Username “admin” Password “admin”
	Normal Exec Level	Username “guest” Password “guest”
	Enable Privileged Exec from Normal Exec Level	Password “super”
	Authentication	local
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)

Function	Parameter	Default
Port Status	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	10/100/1000 Mbps Port Capability	10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Link Aggregation	Static Trunks	none
	LACP (all ports)	Disabled
Spanning Tree Protocol	Status	Enabled (Defaults: All parameters based on IEEE 802.1w)
	Fast Forwarding	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled

Function	Parameter	Default
Class of Service	Ingress Port Priority	0
	Weighted Round Robin	Class 0: 16 Class 1: 64 Class 2: 128 Class 3: 240
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
Multicast Filtering	IGMP Snooping	Enabled
	Act as Querier	Enabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	256 packets per second
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
Jumbo Frames	Status	Disabled

CHAPTER 2
CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 3 "Command Line Interface."

Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting the IP Address" on page 2-11.)

2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Configuring the Logon Password" on page 2-14.)

3. After you enter a user name and password, you will have access to the system configuration program.

Notes: **1.** You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

2. If you log into the Web interface as guest (Normal Exec level), you can view page information but only change the guest password. If you log in as "admin" (Privileged Exec level), you can apply changes on all pages.

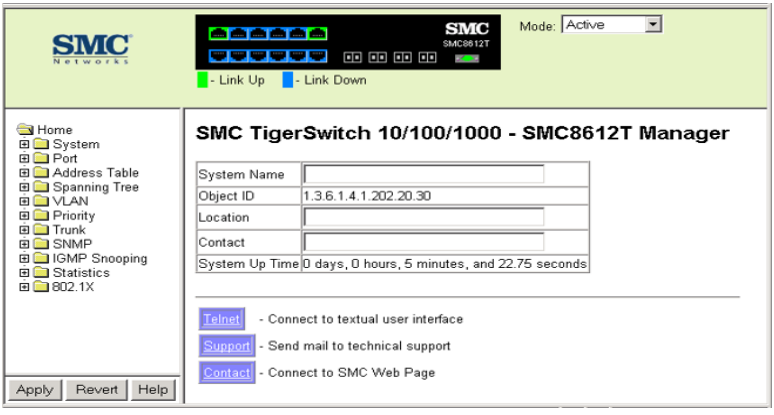
3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Protocol, then you can set the switch port attached to your management station to fast forwarding to improve the switch's response time to management commands issued through the Web interface. (See "STP Port and Trunk Configuration" on page 2-65.)

Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

Home Page

When your Web browser connects with the switch's Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the "Apply" or "Apply Changes" button to confirm the

new setting. The following table summarizes the Web page configuration buttons.

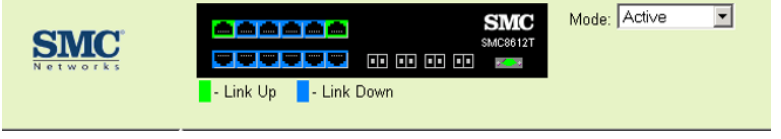
Button	Action
Revert	Cancels specified values and restores current values prior to pressing "Apply" or "Apply Changes."
Refresh	Immediately updates values for the current page.
Apply	Sets specified values to the system.
Apply Changes	Sets specified values to the system.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

Panel Display

The Web agent displays an image of the switch's ports, indicating whether each link is up or down. Clicking on the image of a port opens the Port Configuration page as described on page 2-38.



Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Menu	Description	Page
System		
System Information	Provides basic system description, including contact information	2-8
IP	Sets the IP address for management access	2-11
Passwords	Assigns a new password for the logon user name	2-14
Authentication Settings	Configures RADIUS and TACACS+ authentication parameters	2-16
HTTPS Settings	Configures secure HTTP settings.	2-21
SSH Settings	Configures Secure Shell settings.	2-24
Firmware	Manages code image files	2-26
Configuration	Manages switch configuration files	2-28
Reset	Restarts the switch	
Bridge Extension	Shows the configuration for bridge extension commands; enables GVRP multicast protocol	2-31
Switch Information	Shows the number of ports, hardware/ firmware version numbers, and power status	2-34
Port		
Port Information	Displays port connection status	2-36
Trunk Information	Displays trunk connection status	2-36
Port Configuration	Configures port connection settings	2-38

Menu	Description	Page
Trunk Configuration	Configures trunk connection settings	2-38
Broadcast Storm Protect Configuration	Sets the broadcast storm threshold for each port	2-41
Mirror	Sets the source and target ports for mirroring	2-42
Port Security Action	Configures the port intrusion action globally for the switch	2-45
Port Security Status	Enables port security on specified ports	2-46
Address Table		
Static Addresses	Displays entries for interface, address or VLAN	2-47
Dynamic Addresses	Displays or edits static entries in the Address Table	2-49
Address Aging	Sets timeout for dynamically learned entries	2-51
Spanning Tree		
STP Information	Displays STP values used for the bridge	2-53
STP Configuration	Configures global bridge settings for STP	2-57
STP Port Information	Configures individual port settings for STP	2-61
STP Trunk Information	Configures individual trunk settings for STP	2-61
STP Port Configuration	Configures individual port settings for STP	2-65
STP Trunk Configuration	Configures individual trunk settings for STP	2-65
VLAN		
VLAN Basic Information	Displays basic information on the VLAN type supported by this switch	2-74

Menu	Description	Page
VLAN Current Table	Shows the current port members of each VLAN and whether or not the port supports VLAN tagging	2-75
VLAN Static List	Used to create or remove VLAN groups	2-77
VLAN Static Table	Modifies the settings for an existing VLAN	2-79
VLAN Static Membership by Port	Configures membership type for interfaces including tagged and untagged	2-82
VLAN Port Configuration	Specifies default PVID and VLAN attributes	2-83
VLAN Trunk Configuration	Specifies default trunk VID and VLAN attributes	2-83
Priority		
Default Port Priority	Sets the default priority for each port	2-87
Default Trunk Priority	Sets the default priority for each trunk	2-87
Traffic Class	Maps IEEE 802.1p priority tags to output queues	2-89
Queue Scheduling	Configures Weighted Round Robin queueing	2-92
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both	2-93
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	2-94
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	2-97
Trunk		
LACP Configuration	Allows ports to dynamically join trunks	2-102
Trunk Configuration	Specifies ports to group into static trunks	2-104

Menu	Description	Page
SNMP		
SNMP Configuration	Configures community strings and related trap functions.	2-106
SNMP IP Filtering	Configures IP filtering for SNMP access.	2-110
IGMP		
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	2-113
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID	2-117
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router/switch	2-118
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	2-121
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	2-119
Statistics	Lists Ethernet and RMON port statistics	2-122
802.1X		
802.1X Port Configuration	Sets the authentication mode for individual ports	2-131
802.1X Statistics	Displays protocol statistics for the selected port	2-134

Basic Configuration

Displaying System Information

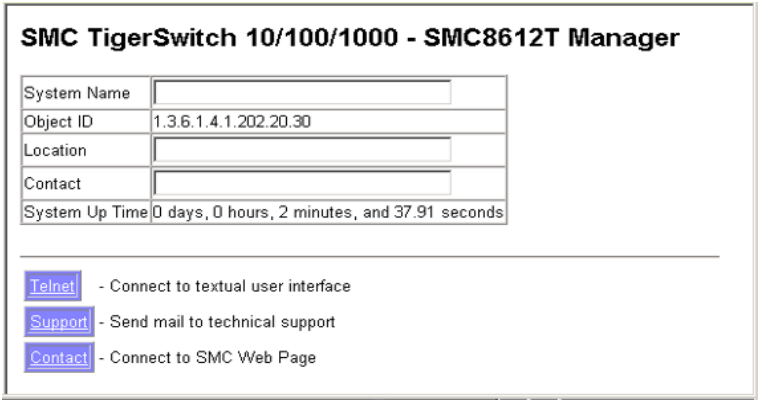
You can easily identify the system by providing a descriptive name, location and contact information.

Command Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.
- **MAC Address*** – The physical layer address for the switch.
- **Web server*** – Shows if management access via HTTP is enabled or disabled.
- **Web server port*** – Shows the TCP port number used by the Web interface.
- **Web secure server*** – Shows if management access via secure HTTP (HTTPS) is enabled or disabled.
- **Web secure server port*** – Shows the TCP port number used by the HTTPS server.
- **POST result*** – Shows results of the power-on self-test

* CLI Only

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows you to access the Command Line Interface via Telnet.)



CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname Test Switch                              3-29
Console(config)#snmp-server location TPS - 3rd Floor              3-66
Console(config)#snmp-server contact Chris                         3-66
Console#show system                                               3-52
System description: SMC Networks SMC8612T
System OID string: 1.3.6.1.4.1.1991.1.5.1.1.4.1.1
System information
 System Up time: 0 days, 2 hours, 4 minutes, and 7.13 seconds
 System Name            : Test Switch
 System Location        : TPS - 3rd Floor
 System Contact         : Chris
 MAC address            : 00-30-f1-47-58-3a
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
Switch Driver Initialization ........... PASS
Switch Internal Loopback Test .......... PASS
------------------- DONE --------------------
Console#
```

Setting the IP Address

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch. If you wish to manually configure IP settings, you need to change the switch's user-specified defaults (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

- **Management VLAN** – This is the only VLAN through which you can gain management access to the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch. However, if other VLANs are configured and you change the Management VLAN, you may lose management access to the switch. In this case, you should reconnect the management station to a port that is a member of the Management VLAN.

- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)

- **IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

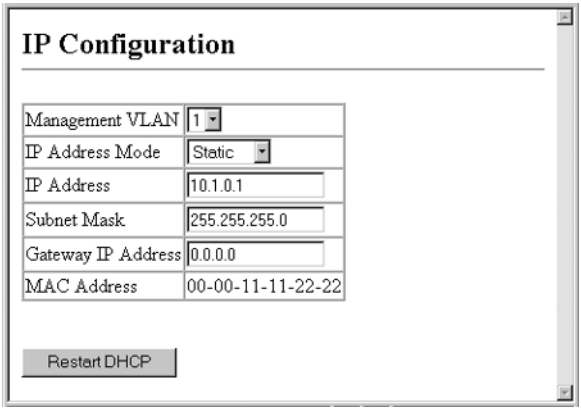
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments.

- **MAC Address** – The MAC address of this switch.

Manual Configuration

Web – Click System, IP. Specify the management interface, IP address and default gateway, then click Apply.



CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1                                    3-92
Console(config-if)#ip address 10.2.13.30 255.255.255.0              3-74
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254                    3-76
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP. Specify the Management VLAN, set the IP Address Mode to DHCP or BOOTP. Then click Apply to save your changes. The switch will broadcast a request for IP configuration settings on the next power reset. Otherwise, you can click Restart DHCP to immediately request a new address.

If you lose your management connection, use a console connection and enter **show ip interface** to determine the new switch address.

CLI – Specify the management interface, and set the IP Address Mode to DHCP or BOOTP.

```
Console(config)#interface vlan 1                                    3-92
Console(config-if)#ip address dhcp                                  3-74
Console(config-if)#end
Console#ip dhcp restart                                             3-75
Console#show ip interface                                           3-77
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the Web interface. You can only restart DHCP service via the Web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                             3-75
```

Security

Configuring the Logon Password

The guest only has read access for most configuration parameters. However, the administrator has write access for parameters governing the onboard agent. You should therefore assign a new

administrator password as soon as possible, and store it in a safe place. (If for some reason your password is lost, you can reload the factory deafults file to restore the default passwords as described in “Troubleshooting Chart” on page A-1.)

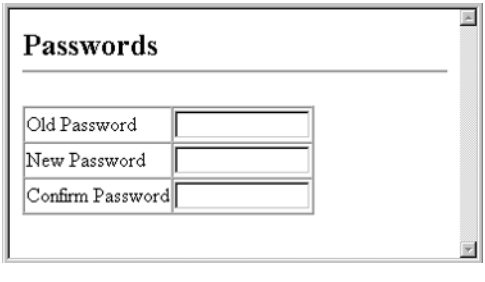
The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.” Note that user names can only be assigned via the CLI.

Command Attributes

- **User Name*** – The name of the user.
  (Maximum length: 8 characters, case sensitive; maximum number of users: 16)
- **Access Level*** – Specifies the user level.
  (Options: 0 - Normal, 15 - Privileged.)
- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, case sensitive)

* CLI only.

Web – Click System, Passwords. To change the password for the current user, enter the old password, then enter the new password, confirm it by entering it again, then click Apply.



CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                    3-30
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring RADIUS/TACACS+ Logon Authentication

You can configure this switch to authenticate users logging into the system for management access using local, RADIUS, or TACACS+ authentication methods.

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS+-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to a switch.

Like RADIUS, Terminal Access Controller Access Control System Plus (TACACS+) is a system that uses a central server to control authentication for access to switches on the network.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol.

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

- RADIUS and TACACS+ logon authentication control management access via the console port, Web browser, or Telnet.

- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **RADIUS** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - **Local** – User authentication is performed only locally by the switch.
  - **[authentication sequence]** – User authentication is performed by up to three authentication methods in the indicated sequence.

RADIUS Settings

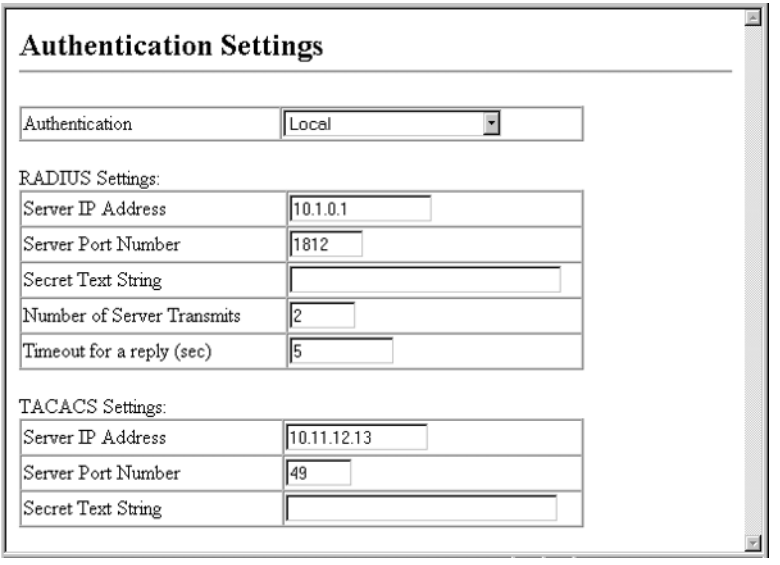
- **Server IP Address** – Address of the RADIUS server. (Default: 10.1.0.1)
- **Server Port Number** – Network (UDP) port of the RADIUS server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Number of Server Transmits** – Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30; Default: 2)
- **Timeout for a reply (secs)** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

TACACS+ Settings

- **Server IP Address** – Address of the TACACS+ server. (Default: 10.1.0.1)
- **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI.

Web – Click System, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.



CLI Commands

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                    3-56
Console(config)#radius-server host 192.168.1.25                3-58
Console(config)#radius-server port 181                         3-58
Console(config)#radius-server key green                        3-59
Console(config)#radius-server retransmit 5                     3-60
Console(config)#radius-server timeout 10                       3-60
Console#show radius-server                                     3-61
Server IP address: 192.168.1.25
 Communication key with radius server: green
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#authentication login tacacs                    3-56
Console(config)#tacacs-server host 10.20.30.40                 3-61
Console(config)#tacacs-server port 200                         3-62
Console(config)#tacacs-server key green                        3-63
Console#show tacacs-server                                     3-63
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's Web interface.

Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port. If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: https://device:port_number.

Note: If you enable HTTPS, you must indicate this in the URL. For example: https://device [:port_number]

The following Web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

* To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 2-23

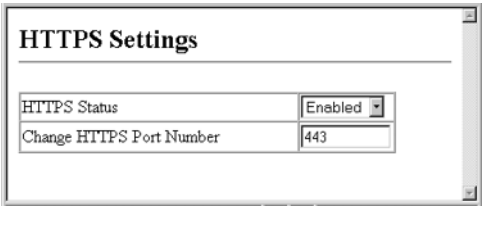
When you start HTTPS, the client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x.

Command Attributes

- **HTTPS Status** — Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)

- **HTTPS Port** — Specifies the UDP port number used for HTTPS/SSL connection to the switch's Web interface. The default is port 443.

Web – Click System, HTTPS Settings. Select Enabled for the HTTPS Status and specify the port number, then click Apply.



CLI Commands

CLI – Enter the following commands to specify the secure port number and to enable HTTPS.

```
Console(config)#ip http secure-server                          3-35
Console(config)#ip http secure-port 441                        3-36
Console(config)#
```

Replacing the Default Secure-site Certificate

When you log onto the Web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Note: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate                            3-21
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type:

```
Console#reload
```

Configuring SSH

The Secure Shell (SSH) server feature provides remote management access via encrypted paths between the switch and SSH-enabled management station clients.

Note: There are two versions of the SSH protocol currently available, SSH v1.x and SSH v2.x. The switch supports only SSH v1.5.

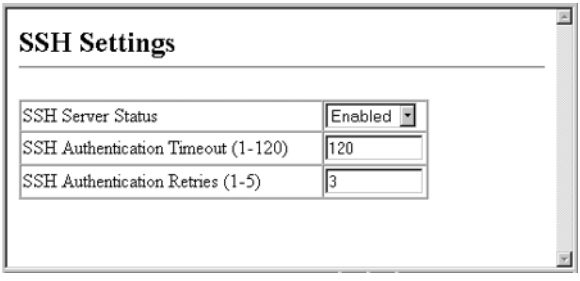
Command Attributes

- **SSH Server Status** — Allows you to enable/disable the SSH server feature on the switch. (Default: enabled)

- **SSH authentication timeout** — Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1 to 120 seconds; Default: 120 seconds)

- **SSH authentication retries** — Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process.
  (Range: 1 to 5 times; Default: 3)

Web – Click System, SSH Settings. Select Enabled for the SSH Server Status, specify the authentication timeout and number of retries, then click Apply.



CLI Commands

CLI – Enter the following commands to configure the SSH service.

```
Console(config)#ip ssh server                                          3-38
Console(config)#ip ssh timeout 100                                     3-37
Console(config)#ip ssh authentication-retries 5                        3-37
Console(config)#
Console#show ip ssh                                                    3-40
Information of secure shell
SSH status: enable
SSH authentication timeout: 100
SSH authentication retries: 5
Console#show ssh                                                       3-40
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   1.5      cipher-3des   session-started
Console#disconnect ssh 0                                               3-39
Console#
```

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

Command Attributes

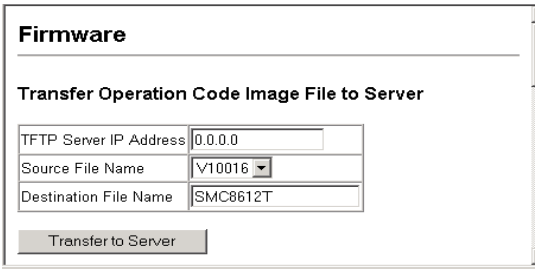
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** — File names are case-sensitive. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of runtime code files is 2.

Downloading System Software from a Server

When downloading runtime code, you can specify the Destination File Name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Transfer from Server.



When you download a file using a different name from the current runtime code file, you need to select the new file name from the drop-down box for the operation code used at startup, and then click Apply Changes.

To start the new firmware, reboot the system.

CLI – Enter the IP address of the TFTP server, select **config** or **opcode** file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file                                          3-21
TFTP server ip address: 10.1.0.99
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: v10.bix
Destination file name: V10000
/
Console#config
Console(config)#boot system opcode: V10000                      3-26
Console(config)#exit
Console#reload                                                  3-18
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch's settings.

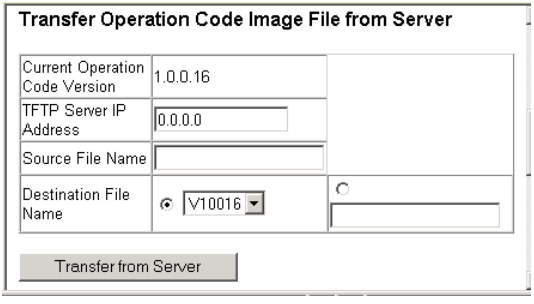
Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** — File names are case-sensitive. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

You can save the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as a destination file name on the switch.

Web – Click System, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.



When you download a file using a different name from the current startup configuration file, you need to select the new file name from from the drop-down box for Startup Operation Code Image File, and press Apply Changes. To use the new settings, reboot the system via the System, Reset menu.

CLI – Enter the IP address of the TFTP server, specify the source file on the server, and set the startup file name on the switch. If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#copy tftp startup-config                                    3-21
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#config
Console(config)#boot system config: startup2.0                      3-26
Console(config)#exit
Console#reload
```

Copying the Running Configuration to a File

You can save the current running configuration to a new file name and then set it as the startup file. Enter a name for the new configuration file, and then click Copy to File.

CLI – If you copy the running configuration to a file, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#copy running-config file                                    3-21
destination file name : 051902.cfg
/
Console#
Console#config
Console(config)#boot system config: 051902.cfg                      3-26
Console(config)#exit
Console#reload                                                      3-18
```

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables, or to configure the global setting for GARP VLAN Registration Protocol (GVRP).

Command Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service Configuration" on page 2-87.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 2-47.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.

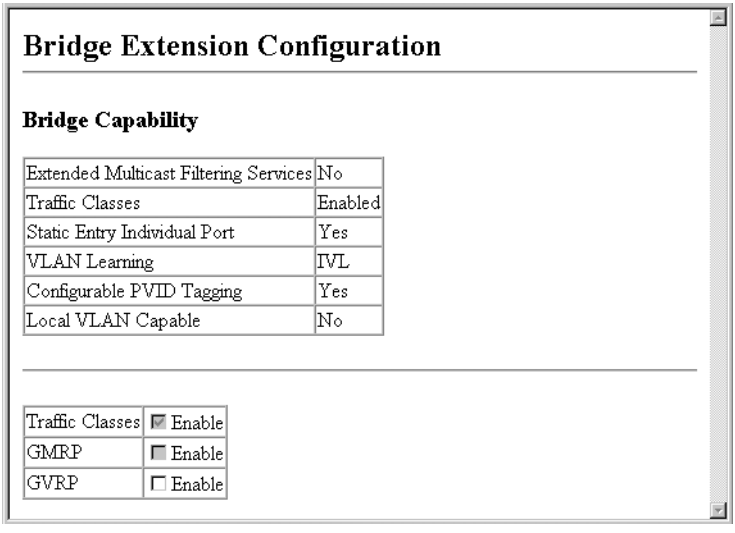
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 2-70.)

- **Local VLAN Capable** – This switch does not support multiple local bridges (i.e., multiple Spanning Trees).

- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

- **GVRP** – GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch.

Web – Click System, Bridge Extension.



Bridge Extension Configuration

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Traffic Classes	☑ Enable
GMRP	☐ Enable
GVRP	☐ Enable

CLI – Enter the following command.

```
Console#show bridge-ext                                          3-147
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

Displaying Switch Hardware/Software Versions

Command Attributes

Main Board

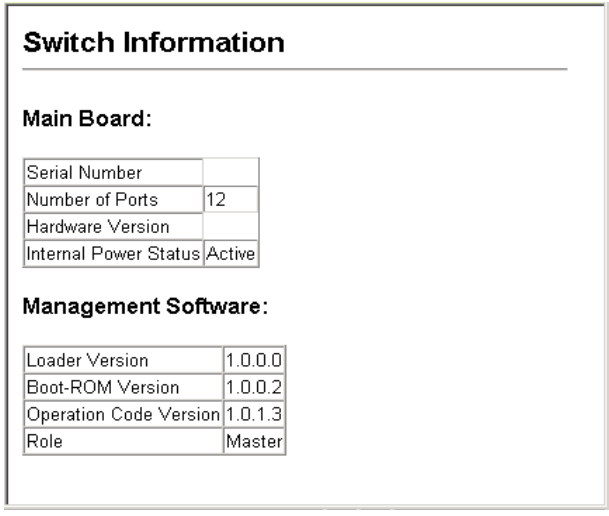
- **Serial Number** – The serial number of the switch.
- **Service Tag*** – Not implemented.
- **Number of Ports** – Number of built-in RJ-45 ports
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.
- **Redundant Power Status*** – Displays the status of the redundant power supply.

* CLI only.

Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version number of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., operating stand-alone).

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	
Number of Ports	12
Hardware Version	
Internal Power Status	Active

Management Software:

Loader Version	1.0.0.0
Boot-ROM Version	1.0.0.2
Operation Code Version	1.0.1.3
Role	Master

CLI – Use the following command to display version information.

```
Console#show version                                          3-54
Unit1
 Serial number           :A217056372
 Service tag             :[NONE]
 Hardware version        :R0C
 Number of ports         :12
 Main power status       :up
 Redundant power status  :not present
Agent(master)
 Unit id                 :1
 Loader version          :1.0.0.0
 Boot rom version        :1.0.0.0
 Operation code version  :2.0.0.19
Console#
```

Port Configuration

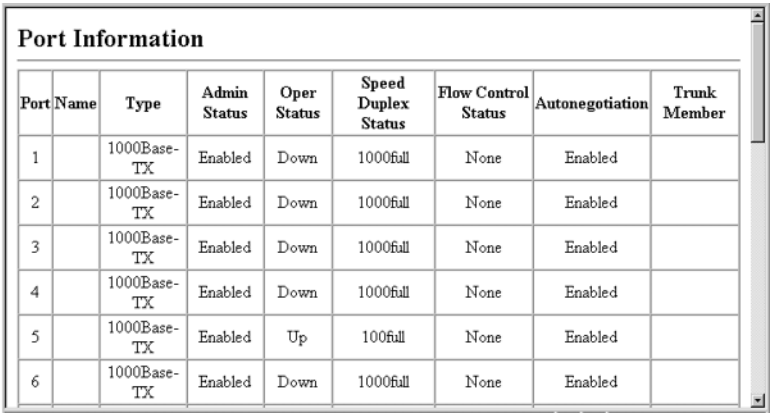
Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Command Attributes

- **Name** – Interface label.
- **Type** – Indicates the of port type (1000Base-TX or 1000Base-SFP).
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed/Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Indicates the type of flow control currently in use.
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Trunk Member** – Shows if port is a trunk member. (Port Information only.)
- **Creation** – Shows if a trunk is manually configured or dynamically set via LACP. (Trunk Information only.)

Web – Click Port, Port Information or Trunk Information. Modify the required interface settings, and click Apply.



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		1000Base-TX	Enabled	Down	1000full	None	Enabled	
2		1000Base-TX	Enabled	Down	1000full	None	Enabled	
3		1000Base-TX	Enabled	Down	1000full	None	Enabled	
4		1000Base-TX	Enabled	Down	1000full	None	Enabled	
5		1000Base-TX	Enabled	Up	100full	None	Enabled	
6		1000Base-TX	Enabled	Down	1000full	None	Enabled	

CLI – This example shows the connection status for Port 13.

```
Console#show interfaces status ethernet 1/13                    3-103
Information of Eth 1/13
 Basic information:
  Port type: 1000T
  Mac address: 00-00-11-11-22-2F
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
```

Configuring Interface Connections

You can use the Trunk Configuration or Port Configuration page to enable/disable an interface, manually fix the speed and duplex mode, set flow control, set auto-negotiation, and set the interface capabilities to advertise.

Command Attributes

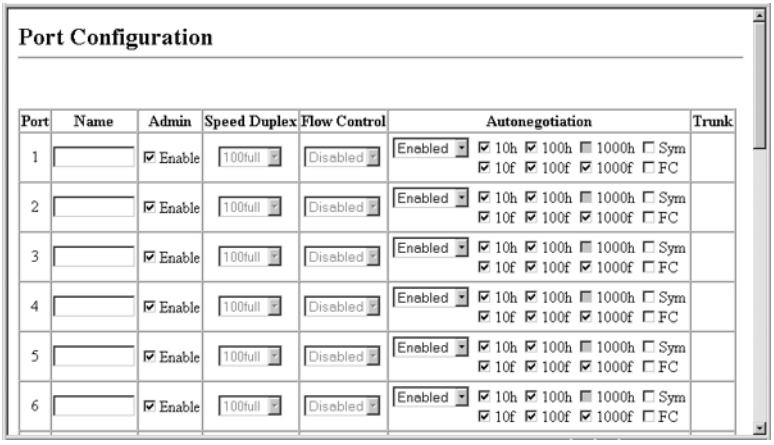
- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows manual selection of port speed and duplex mode (i.e., with auto-negotiation disabled).
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation/Port Capabilities** – Allows auto-negotiation to be enabled/disabled. Specifies the capabilities to be advertised for a port during auto-negotiation. The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation

- **Sym (Gigabit only)** – Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames.(The current switch chip only supports symmetric pause frames.)
- **FC** - Supports flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)
  (Default: Autonegotiation enabled; Advertised capabilities for 100BASE-TX – 10half, 10full, 100half, 100full; 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full)

- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see "Port Trunk Configuration" on page 2-100.

Note: Autonegotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.



Port Configuration

Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation	Trunk
1		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	
2		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	
3		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	
4		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	
5		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	
6		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                          3-92
Console(config-if)#description RD SW#13                          3-93
Console(config-if)#shutdown                                      3-99
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                3-95
Console(config-if)#speed-duplex 100half                          3-94
Console(config-if)#flowcontrol                                   3-97
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                          3-96
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

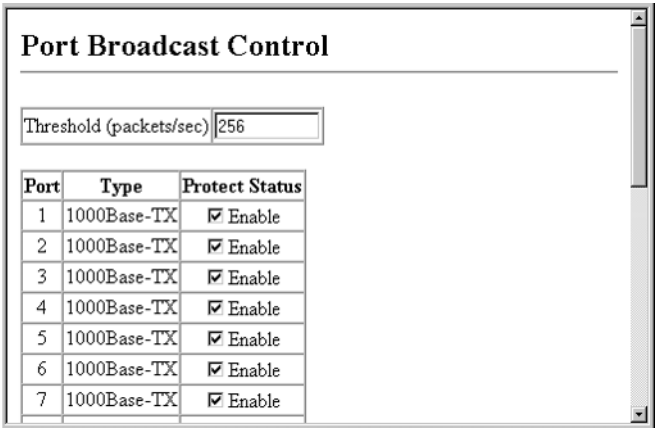
Command Usage

- Broadcast Storm Control is enabled by default.
- The default threshold is 256 packets per second.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to all ports on the switch.

Command Attributes

- Threshold – Threshold as percentage of port bandwidth. (Range: 16, 64, 128, or 256 packets per second; Default: 256 packets per second)
- Broadcast Control Status – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)

Web – Click Port, Port Broadcast Control. Set the threshold for all ports, and then click Apply.



CLI – Specify the required interface, and then enter the threshold. The following sets broadcast suppression at 128 packets per second on port 1.

```
Console(config)#interface ethernet 1/1                          3-92
Console(config-if)#switchport broadcast packet-rate 128         3-100
Console(config-if)#
```

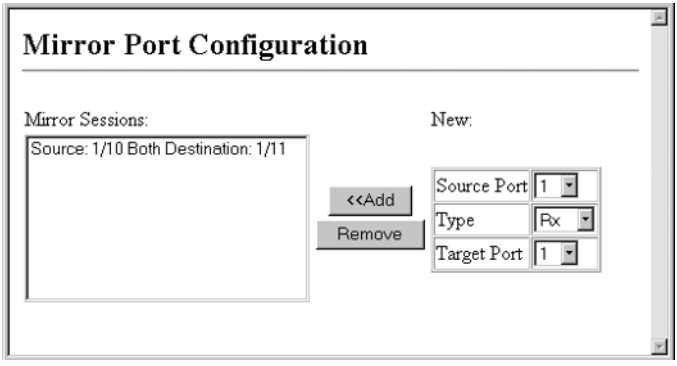
Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Command Usage

- The mirror port and monitor port speeds must match, otherwise traffic may be dropped from the monitor port.
- The switch supports only one port mirror session.

Web – Click Port, Mirror. Specify the source port, the traffic type to be mirrored, and the target port, then click Add.



CLI – Use the interface command to select the target port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10                    3-92
Console(config-if)#port monitor ethernet 1/11              3-174
Console(config-if)#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.

Note that a secure port has the following restrictions:

- It should not be connected to a network interconnection device.
- It cannot be configured as a member of a static trunk.

- It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.

Note: A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.

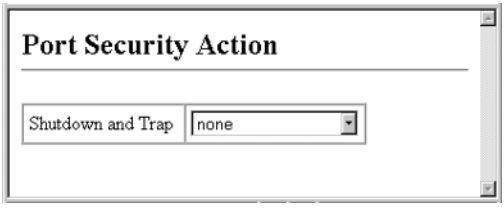
Port Security Action

The switch allows you to set the security action to be taken when a port intrusion is detected. This setting applies to all ports on the switch.

- **Shutdown and Trap** — Indicates the action to be taken when a port security violation is detected:

  - **None**: Indicates that no action should be taken. (This is the default.)
  - **Trap and Shutdown**: Indicates that the port is to be disabled and an SNMP trap message sent.

Web – Click Port, Port Security Action. Specify the security action for a port intrusion, then click Apply.



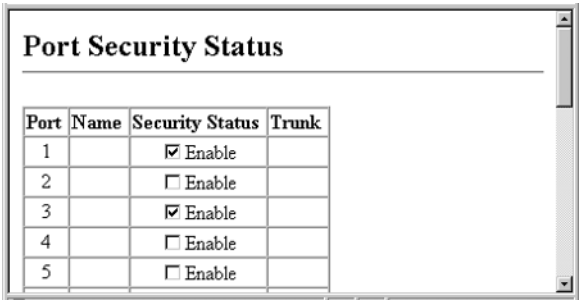
Port Security Configuration

On the Port/Port Security Status page, you can enable/disable security for any switch port. For each port number listed in the "Port" column, you can configure the following parameter:

- **Security Status** — Enables or disables port security on the port. (Default: disabled)

Note: If a port is disabled due to a security violation, it must be manually re-enabled from the Port/Port Configuration page.

Web – Click Port, Port Security Status. Check the checkbox in the Security Status column to enable security for a port, then click Apply.



CLI – Use the interface command to select the target port, then use the port security action command to configure the port intrusion action (applies to all ports). Use the port security command to enable security for the port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown     3-101
Console(config-if)#port security
Console(config-if)#
```

Address Table Settings

Switches store the addresses for all known devices. This information is used to route traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

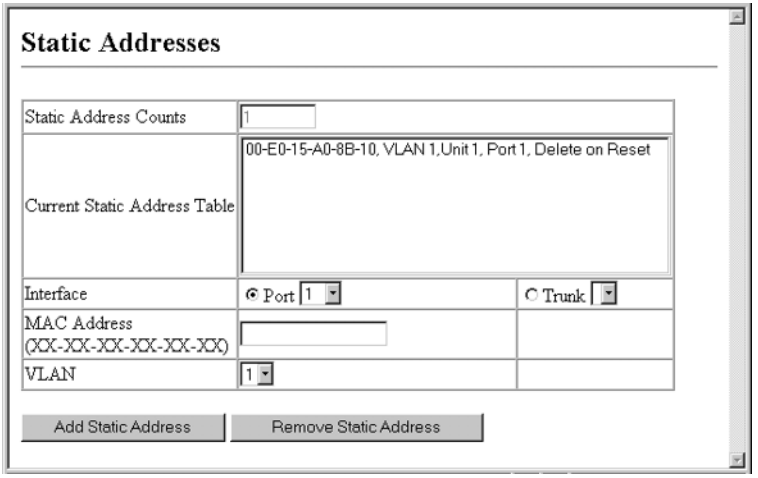
Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Usage

Entries specified via the Web interface are permanent. Entries specified via the CLI can be made permanent or can be set to be deleted on reset.

Web – Click Address able, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.



CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table address 00-e0-29-94-34-de
ethernet 1/1 vlan 1 delete-on-reset                          3-108
Console(config)#
```

Displaying the Address Table

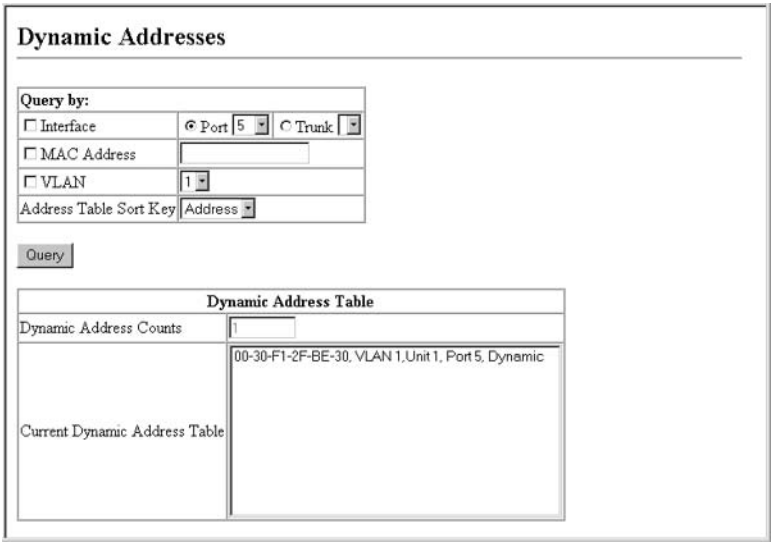
The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address is forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Usage

- You can display entries in the dynamic address table by selecting an interface (either port or trunk), MAC address, or VLAN.
- You can sort the information displayed based on interface (port or trunk), MAC address, or VLAN.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., Interface, MAC Address, or VLAN), the method of sorting the displayed addresses, then click Query.

For example, the following screen shows the dynamic addresses for port 5.



CLI – This example displays the address table entries for port 11.

```
Console#show mac-address-table interface ethernet 1/11        3-109
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- ----------------
  Eth 1/11 00-10-b5-62-03-74    1 Learned
Console#
```

Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Usage

The range for the aging time is 17 - 2184 seconds. (The default is 300 seconds.)

Web – Click Address Table, Address Aging. Specify the new aging time, then click Apply.

CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400              3-111
Console(config)#
```

Spanning Tree Protocol Configuration

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (i.e., an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down.

The Spanning Tree Protocols supported by the switch include the following standards:

- **STP** – Spanning Tree Protocol (IEEE 802.1D).
- **RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w).

STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves much faster reconfiguration (around one tenth of that required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

STP Information

The Spanning Tree, STP Information page contains information on the current status of the Spanning Tree.

Command Attributes

- **Spanning Tree State** — Indicates if the Spanning Tree Protocol is currently enabled on the switch.
- **Bridge ID** — Identifies a unique identifier for the switch in the Spanning Tree. The ID is calculated using the defined Spanning Tree priority of the switch and its MAC address. The lower the Bridge ID, the more likely the switch will act as the root.
- **Max Age** — The maximum time (in seconds) the switch can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STP information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)
- **Hello Time** — Specifies the time interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** — The maximum time (in seconds) the switch will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- **Designated Root** — Identifies the priority and MAC address of the device in the Spanning Tree that the switch has accepted as the root device.

  - **Root Port** — Specifies the port number on the switch that is closest to the root. The switch communicates with the root device through this port. If there is no root port, the switch has been accepted as the root device of the Spanning Tree network.
  - **Root Path Cost** — Identifies the path cost from the root port on the switch to the root device.

  - **Root Hello Time*** – Interval (in seconds) at which this device transmits a configuration message.

  - **Root Maximum Age*** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

  - **Root Forward Delay*** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

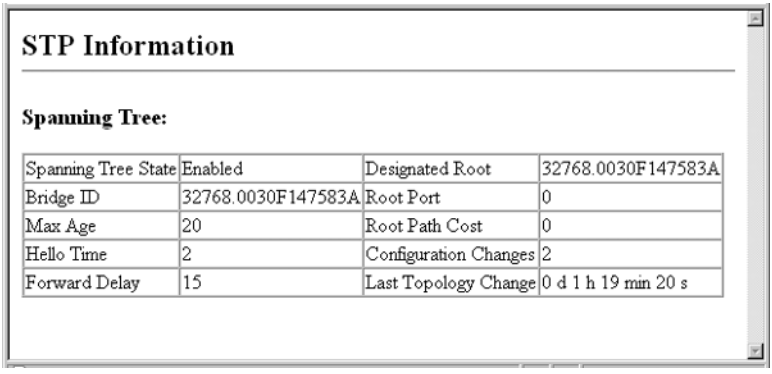
  - **Root Hold Time*** – The interval (in seconds) during which no more than two bridge configuration protocol data units shall be transmitted by this node.

- **Configuration Changes** — Specifies the number of times the Spanning Tree has been reconfigured.

- **Last Topology Change** — Identifies the time since the Spanning Tree was last reconfigured.

* CLI only.

Web – Click Spanning Tree, STP Information to display current Spanning Tree information.



STP Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0030F147583A
Bridge ID	32768.0030F147583A	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 1 h 19 min 20 s

CLI – This example shows the current Spanning Tree settings.

```
Console#show spanning-tree                                        3-128
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.000011112222
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :1
 Last topology changes time (sec.):10811
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.1
 Designated root      : 32768.000011112222
 Designated bridge    : 32768.000011112222
 Fast forwarding      : disable
 Forward transitions  : 0
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point

Eth  1/ 2 information
---------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 10000
-
-
-
-
-

Console#
```

STP Configuration

Global settings apply to the entire switch.

Command Usage

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- **STP Mode** – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

- **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Command Attributes

- **Spanning Tree State** — Enables or disables the Spanning Tree. If you enable the Spanning Tree, you must complete the other fields. (Default: enabled)

- **Spanning Tree Type** — Specifies the type of Spanning Tree Protocol used on the switch: (Default: RSTP)

  - **STP**: Spanning Tree Protocol (IEEE 802.1D; i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode))
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)

- **Priority** — Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

- **Hello Time** — Interval (in seconds) at which the switch transmits a configuration message.

  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

- **Maximum Age** — The maximum time (in seconds) the switch can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

- **Forward Delay** — The maximum time (in seconds) the switch will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

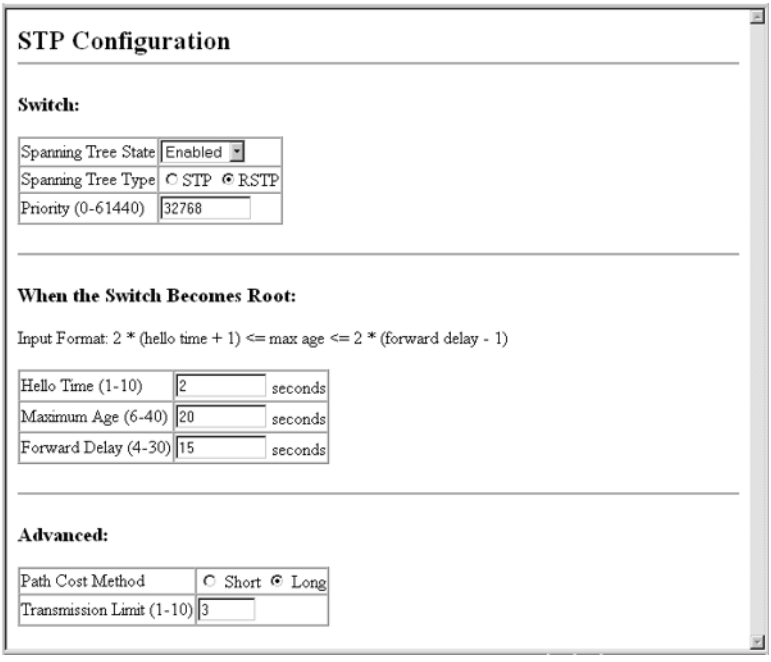
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

- **Path Cost Method** — The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

  - **Long**: Specifies 32-bit based values that range from 1-200,000,000.
  - **Short**: Specifies 16-bit based values that range from 1-65535. (This is the default.)

- **Transmission Limit** — The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Web – Click Spanning Tree, STP Configuration. Modify the required attributes, then click Apply.



CLI – This example enables Spanning Tree Protocol, and then sets the indicated attributes.

```
Console(config)#spanning-tree mode rstp                          3-115
Console(config)#spanning-tree                                    3-114
Console(config)#spanning-tree forward-time 15                    3-116
Console(config)#spanning-tree hello-time 2                       3-117
Console(config)#spanning-tree max-age 20                         3-118
Console(config)#spanning-tree priority 40000                     3-119
Console(config)#spanning-tree pathcost method long               3-120
Console(config)#spanning-tree transmission-limit 5               3-121
Console(config)#
```

STP Port and Trunk Information

The Spanning Tree, STP Port Information and Spanning Tree, STP Trunk Information display the current status of ports and trunks in the Spanning Tree.

Command Attributes

- **STP Status** — Displays current state of this port within the Spanning Tree:

  - **Discarding** — Port receives STP configuration messages, but does not forward packets.
  - **Learning** — Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** — Port forwards packets, and continues learning addresses.

  The rules defining port status are:

  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.

- **Designated Cost** — The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

- **Designated Bridge** — The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

- **Designated Port** — The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for "Admin Link Type" in the STP Port/Trunk Configuration page.

- **Oper Edge Port** – This parameter is initialized to the setting for "Admin Edge Port" in the STP Port/Trunk Configuration page (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.

- **Port Role** – Roles are assigned according to whether the port is part of the active Spanning Tree topology:

  - **Root:** The port is connecting the bridge to the root bridge.
  - **Designated:** The port is connecting a LAN through the bridge to the root bridge.
  - **Alternate** or **Backup:** A port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.
  - **Disabled:** The role is set to disabled if a port has no role within the Spanning Tree.

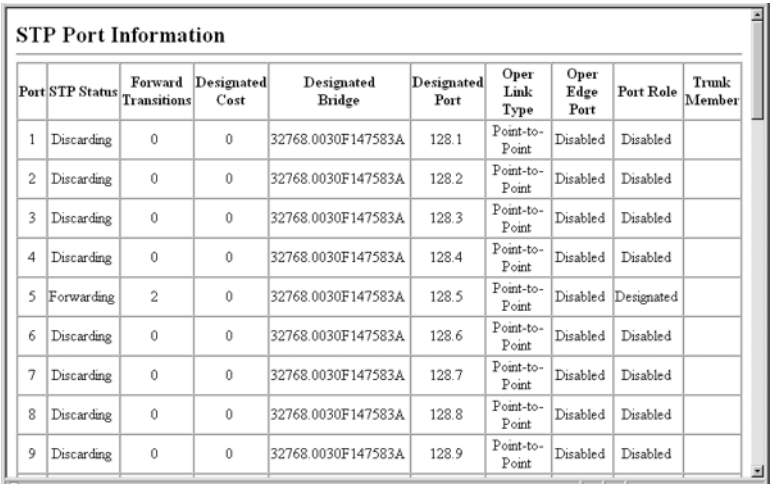
- **Trunk Member** — Indicates whether the port is configured as a trunk member. (STP Port Information page only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if STA has been enabled on this interface.
- **Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.
- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Link Type** – The link type attached to this interface.
  - **Point-to-Point** – A connection to exactly one other bridge.
  - **Shared** – A connection to two or more bridges.
  - **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

Web – Click Spanning Tree, STP Port Information or STP Trunk Information.



STP Port Information

Port	STP Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Discarding	0	0	32768.0030F147583A	128.1	Point-to-Point	Disabled	Disabled	
2	Discarding	0	0	32768.0030F147583A	128.2	Point-to-Point	Disabled	Disabled	
3	Discarding	0	0	32768.0030F147583A	128.3	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0030F147583A	128.4	Point-to-Point	Disabled	Disabled	
5	Forwarding	2	0	32768.0030F147583A	128.5	Point-to-Point	Disabled	Designated	
6	Discarding	0	0	32768.0030F147583A	128.6	Point-to-Point	Disabled	Disabled	
7	Discarding	0	0	32768.0030F147583A	128.7	Point-to-Point	Disabled	Disabled	
8	Discarding	0	0	32768.0030F147583A	128.8	Point-to-Point	Disabled	Disabled	
9	Discarding	0	0	32768.0030F147583A	128.9	Point-to-Point	Disabled	Disabled	

CLI – This example displys the current Spanning Tree status of a port.

```
Console#show spanning-tree ethernet 1/5                          3-128
Eth  1/ 5 information
---------------------------------------------------------------
 Admin status          : enable
 Role                  : designate
 State                 : forwarding
 Path cost             : 100000
 Priority              : 128
 Designated cost       : 0
 Designated port       : 128.5
 Designated root       : 32768.000011112222
 Designated bridge     : 32768.000011112222
 Fast forwarding       : disable
 Forward transitions   : 1
 Admin edge port       : disable
 Oper edge port        : disable
 Admin Link type       : auto
 Oper Link type        : point-to-point

Console#
```

STP Port and Trunk Configuration

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

Command Attributes

- **STP State** — Displays current state of this port within the Spanning Tree:

  - **Discarding** — Port receives STP configuration messages, but does not forward packets.
  - **Learning** — Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** — Port forwards packets, and continues learning addresses.

- **Priority** — Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)

- **Path Cost** — This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)

  - Range —
    Ethernet: 200,000-20,000,000
    Fast Ethernet: 20,000-2,000,000
    Gigabit Ethernet: 2,000-200,000
  - Defaults —
    Ethernet — half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
    Fast Ethernet — half duplex: 200,000; full duplex: 100,000; trunk: 50,000
    Gigabit Ethernet — full duplex: 10,000; trunk: 5,000

Note: When the Path Cost Method is set to short, the maximum path cost is 65,535.

- **Admin Link Type** — The link type attached to this interface. (Default: Auto)

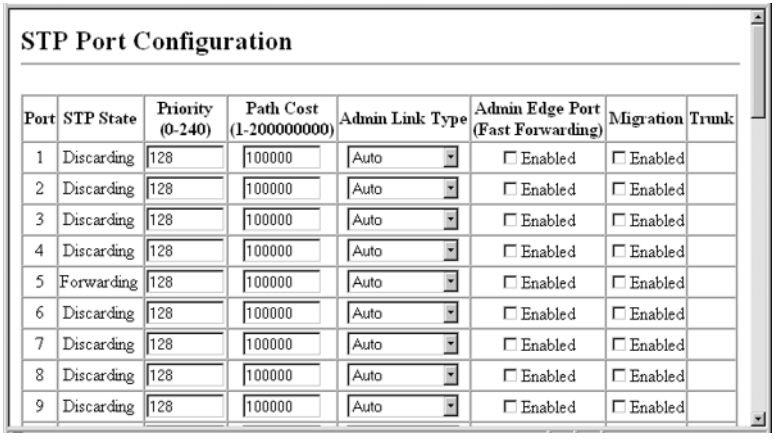
  - **Point-to-Point** — A connection to exactly one other bridge.
  - **Shared** — A connection to two or more bridges.
  - **Auto** — The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

- **Admin Edge Port** — You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the Spanning Tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the Spanning Tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

- **Migration** — Re-checks the appropriate BPDU format to send on the selected interface. If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also check this Migration check box to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces.

- **Trunk** – Specifies if a port is member of a trunk.

Web – Click Spanning Tree, STP Port Configuration or STP Trunk Configuration. Modify the required attributes, then click Apply.



STP Port Configuration

Port	STP State	Priority (0-240)	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
2	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
3	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
4	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
5	Forwarding	128	100000	Auto	☐ Enabled	☐ Enabled	
6	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
7	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
8	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
9	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	

CLI – This example sets STP attributes for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 128          3-123
Console(config-if)#spanning-tree cost 19                    3-122
Console(config-if)#spanning-tree link-type auto             3-127
Console(config-if)#no spanning-tree edge-port               3-125
Console#spanning-tree protocol-migration ethernet 1/5       3-126
Console#
```

VLAN Configuration

In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q-compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs

- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port. But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by using a Layer-3 router or switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each endstation should be assigned. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these

hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on ports to prevent advertisements being propagated, or forbid ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you must configure static VLANs for the switch ports connected to these devices. You also still need to enable GVRP on these edge switches, as well as on the core switches in the network.

Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you need to create a VLAN for that group and enable tagging on all ports.

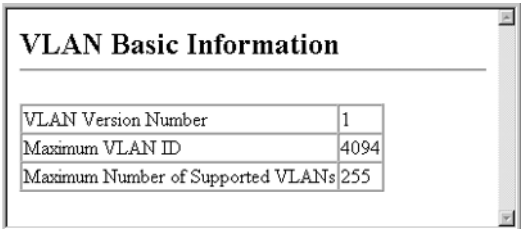
Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Displaying Basic VLAN Information

Command Attributes

- **VLAN Version Number** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard. (Web interface only.)
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

Web – Click VLAN, VLAN Basic Information.



CLI – Enter the following command.

```
Console#show bridge-ext                                          3-147
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

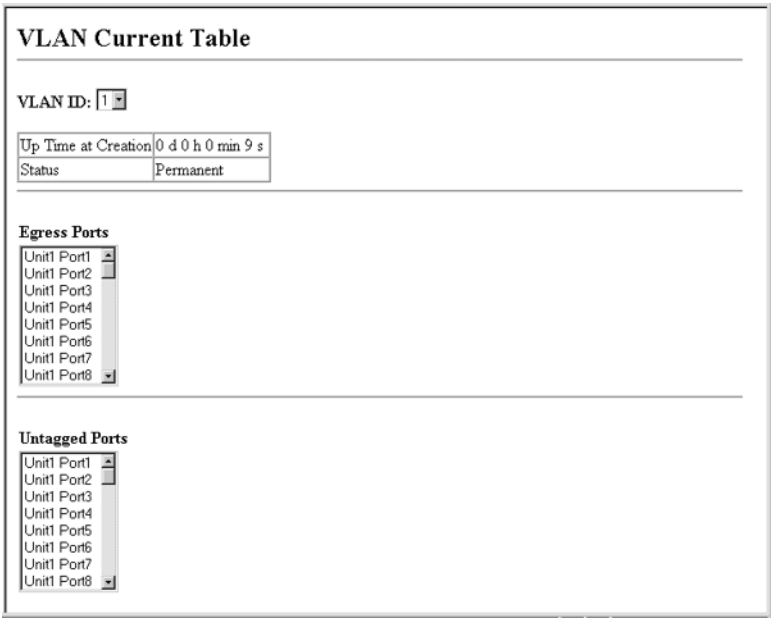
Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes for Web Interface

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Up Time at Creation** – Time this VLAN was created; i.e., System Up Time.
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Tagged Ports** – Shows the tagged VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members

Web – Click VLAN, VLAN Current Table. Select any ID from the scroll-down list.



Command Attributes for CLI Interface

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).

- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                                    3-140
VLAN   Type     Name            Status  Ports/Channel groups
----   ------- --------------- --------- -----------------------------------
   1   Static   DefaultVlan     Active  Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth110
                                        Eth1/11 Eth1/12

Console#
```

Creating VLANs

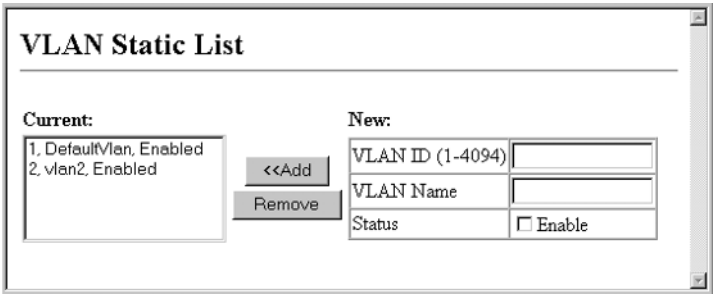
Use The VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).

- **Status** – Shows if this VLAN is enabled or disabled (Web).
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **State** – Shows if this VLAN is enabled or disabled (CLI).
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, VLAN Static List. Enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.



CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                    3-131
Console(config-vlan)#vlan 5 name R&D media ethernet state active3-132
Console(config-vlan)#
```

Adding Interfaces Based on Membership Type

Use the VLAN Static Table to modify the settings for an existing VLAN. You can add or delete port members for a VLAN, disable or enable VLAN tagging for any port, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Note that VLAN 1 is the default untagged VLAN containing all ports on the switch, and cannot be modified via this page.)

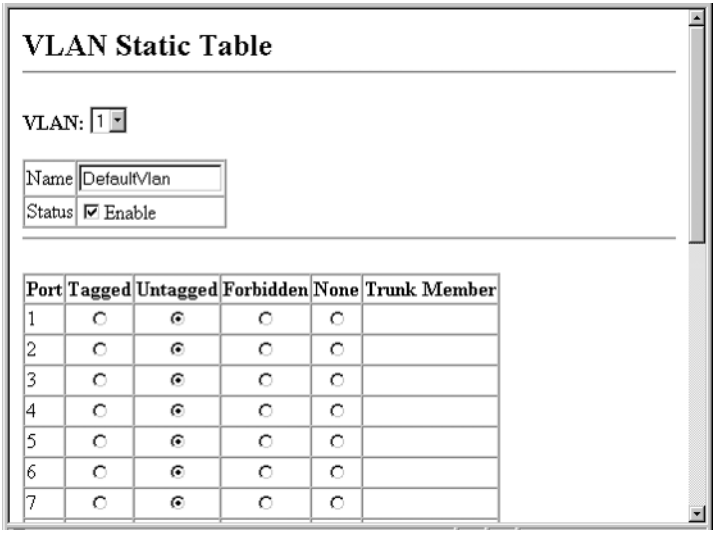
You can use the VLAN Static Table to assign ports to the specified VLAN group as an IEEE 802.1Q tagged port. Assign ports as tagged if they are connected to 802.1Q VLAN-compliant devices. If the port is connected to VLAN-unaware devices, frames will be passed to the untagged VLAN group this port has been assigned to under the VLAN Port Configuration page.

Command Attributes

- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.

- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface s forbidden from automatically joining the VLAN via GVRP. For more information, see "GVRP" on page 81.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, VLAN Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.



CLI – The following example shows how to add tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                          3-92
Console(config-if)#switchport allowed vlan add 2 tagged         3-138
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

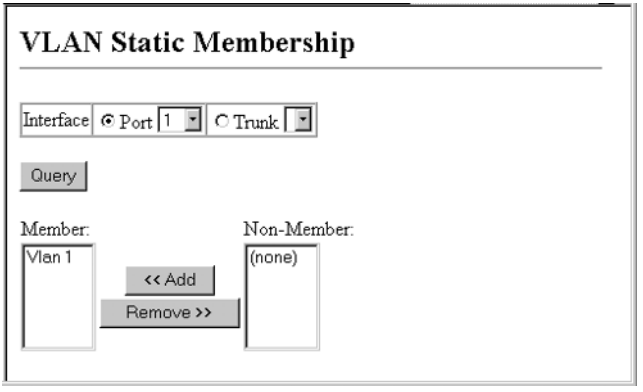
Adding Interfaces Based on Static Membership

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface add an interface to the selected VLAN as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, VLAN Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display VLAN membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.



CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                          3-92
Console(config-if)#switchport allowed vlan add 1 tagged         3-138
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.

- **GARP** – Group Address egistration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)

- **Ingress Filtering** – If ingress filtering is enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port. (Default: Disabled)

  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled, the interface will flood incoming frames for VLANs which do not include this ingress port in their member set (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled, the interface will discard incoming frames tagged for VLANs which do not include this ingress port in their member set.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.

- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See "Displaying Bridge Extension Capabilities" on page 2-31.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Enabled)

- **GARP Join Timer*** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

- **GARP Leave Timer*** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

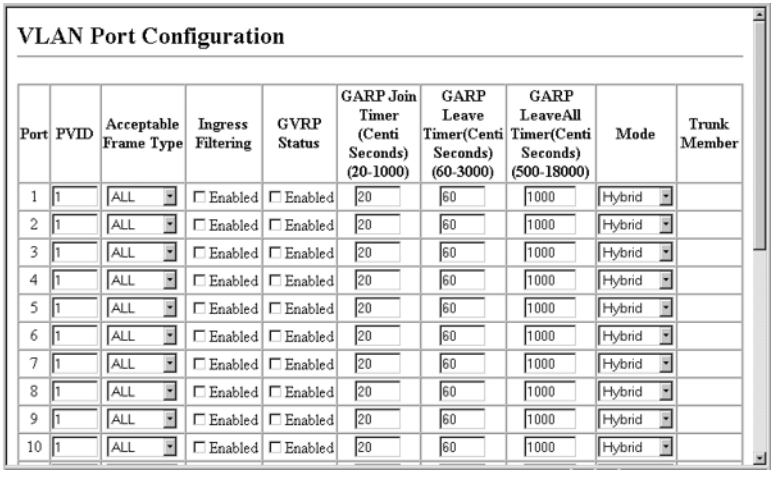
- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
(Range: 500-18000 centiseconds; Default: 1000)

* GARP timer settings must follow this rule:
2 x (join timer) < leave timer < leaveAll timer

- **Mode** – Indicates VLAN membership mode for a port. (Configure via CLI, see page 3-134.)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may receive or transmit tagged or untagged frames.

- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, VLAN Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.



VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer(Centi Seconds) (60-3000)	GARP LeaveAll Timer(Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
2	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
3	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
4	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
5	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
6	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
7	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
8	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
9	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
10	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	

CLI – This example sets port 1 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/1                          3-92
Console(config-if)#switchport acceptable-frame-types tagged     3-135
Console(config-if)#switchport ingress-filtering                 3-136
Console(config-if)#switchport native vlan 3                     3-137
Console(config-if)#switchport gvrp                              3-142
Console(config-if)#garp timer join 10                           3-144
Console(config-if)#garp timer leave 90                          3-144
Console(config-if)#garp timer leaveall 2000                     3-144
Console(config-if)#switchport mode hybrid                       3-134
Console(config-if)#
```

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

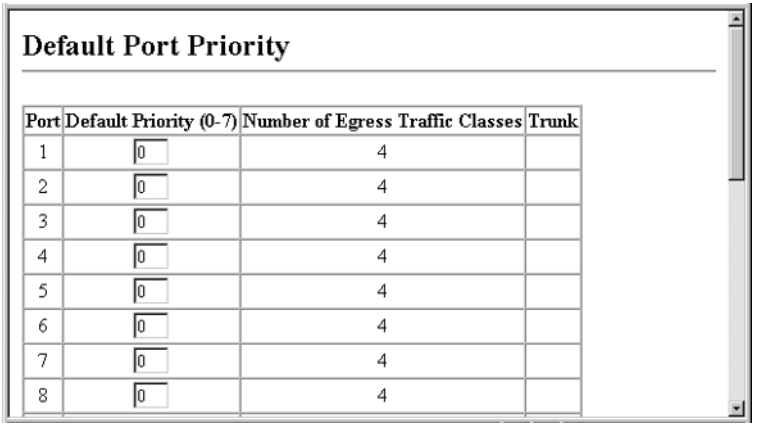
Command Usage

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies if the incoming frame is an untagged frame received from a VLAN trunk or a static-access port. This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority** – The priority that is assigned to untagged frames received on the specified port. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.



Default Port Priority

Port	Default Priority (0-7)	Number of Egress Traffic Classes	Trunk
1	0	4	
2	0	4	
3	0	4	
4	0	4	
5	0	4	
6	0	4	
7	0	4	
8	0	4	

CLI – This example assigns a default priority or 5 to port 3.

```
Console(config)#interface ethernet 1/3                          3-92
Console(config-if)#switchport priority default 5                3-161
```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

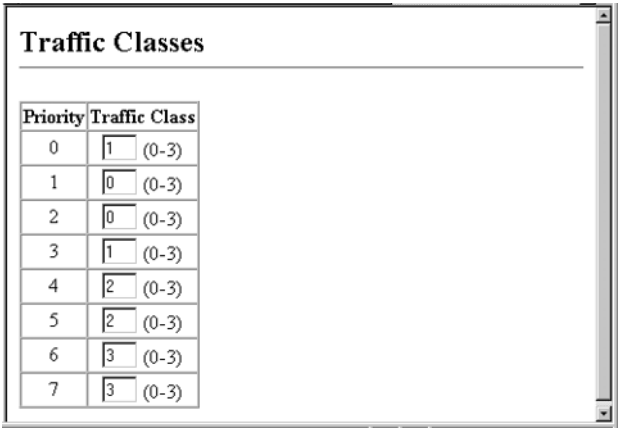
	Queue			
	0	**1**	**2**	**3**
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

- **Priority** – CoS value. (Range: 0 to 7, where 7 is the highest priority)
- **Traffic Class** – Output queue buffer. (Range: 0 - 3, where 3 is the highest CoS priority queue)

Web – Click Priority, Traffic Classes. Assign priorities to the output queues, then click Apply.



CLI – The following example shows how to map CoS values 0, 1 and 2 to CoS priority queue 0, value 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3.

```
Console(config)#interface ethernet 1/1                          3-92
Console(config)#queue cos-map 0 0 1 2                           3-163
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet 1/1                         3-166
Information of Eth 1/1
 Queue ID Traffic class
 -------- -------------
    0     0 1 2
    1     3
    2     4 5
    3     6 7
Console#
```

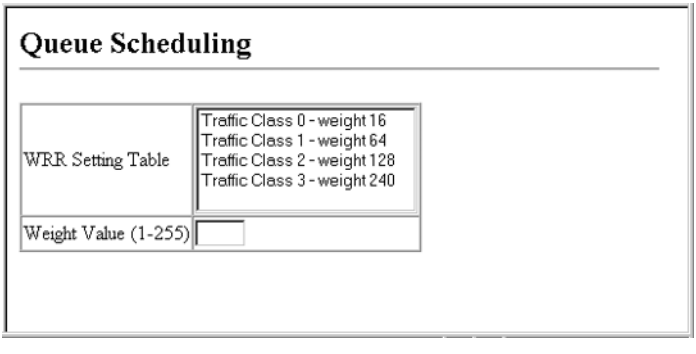
Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in "Mapping CoS Values to Egress Queues" on page 2-89, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table** – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Set a new weight for the selected traffic class.

Web – Open Priority, Queue Scheduling. Select a traffic class by clicking on it with your cursor, enter a weight value, and then click Apply.


Queue Scheduling
WRR Setting Table
Traffic Class 0 - weight 16
Traffic Class 1 - weight 64
Traffic Class 2 - weight 128
Traffic Class 3 - weight 240
Weight Value (1-255)

CLI – The following example shows how to assign WRR weights of 1, 4, 16 and 64 to the CoS priority queues 0, 1, 2 and 3.

```
Console(config)#queue bandwidth 1 4 16 64                    3-162
Console(config)#exit
Console#show queue bandwidth                                 3-165
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

Mapping Layer 3/4 Priorities to CoS Values

This switch supports a common method of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet. The ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Precedence or DSCP Priority and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.
- IP Precedence and DSCP Priority settings are global and apply to all ports on the switch.

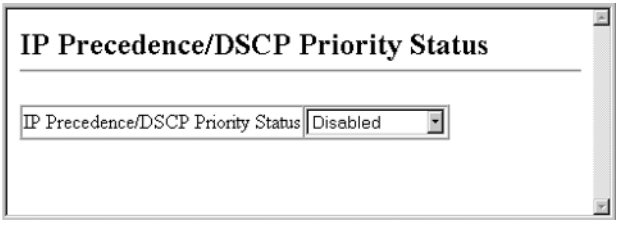
Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **IP Precedence/DSCP Priority Status** – Selects IP Precedence, DSCP, or disables both priority services.

Web – Click Priority, IP Precedence Priority. Select IP Precedence or IP DSCP from the IP Precedence, DSCP Priority Status menu.



CLI – The following example globally enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                                    3-166
Console#
```

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for

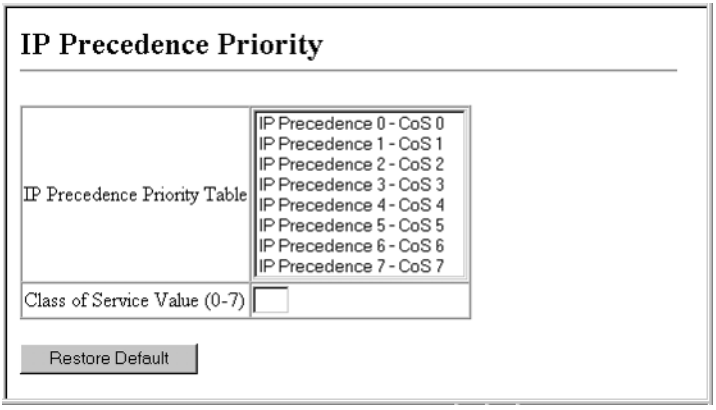
network control, and the other bits for various application types. ToS bits are defined in the following table.

Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precendence value. Note that "0" represents low priority and "7" represent high priority.

Web – Click Priority, IP Precedence Priority. Select an IP Precedence value from the IP Precedence Priority Table by clicking on it with your cursor, enter a value in the Class of Service Value field, and then click Apply. Be sure to also select IP Precedence from the IP Precedence/DSCP Priority Status menu.


IP Precedence Priority
IP Precedence Priority Table
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7
Class of Service Value (0-7)
Restore Default

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 on port 5, and then displays all the IP Precedence settings for that port. (Note that the setting is global and applies to all ports on the switch.)

```
Console(config)#map ip precedence                                  3-166
Console(config)#interface ethernet 1/5                             3-92
Console(config-if)#map ip precedence 1 cos 0                       3-167
Console(config-if)#end
Console#show map ip precedence ethernet 1/5                        3-171
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   0
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, and it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note

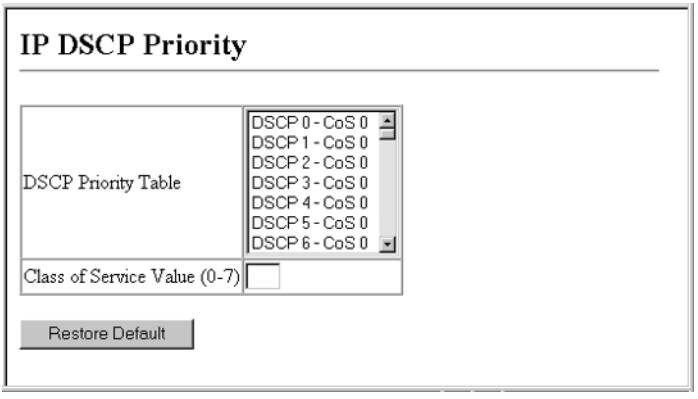
that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that "0" represents low priority and "7" represent high priority.

Web – Click Priority, IP DSCP Priority. Select a DSCP priority value from the DSCP Priority Table by clicking on it with your cursor, enter a value in the Class of Service Value field, and then click Apply. Be sure to also select IP DSCP from the IP Precedence/ DSCP Priority Status menu.


IP DSCP Priority
DSCP Priority Table
DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
Class of Service Value (0-7)
Restore Default

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 1 to CoS value 0 on port 5, and then displays all the DSCP Priority settings for that port. (Note that the setting is global and applies to all ports on the switch.)

```
Console(config)#map ip dscp                                    3-169
Console(config)#interface ethernet 1/5                         3-92
Console(config-if)#map ip dscp 1 cos 0                         3-170
Console(config-if)#end
Console#show map ip dscp ethernet 1/5                          3-172
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 5    0   0
  Eth 1/ 5    1   0
  Eth 1/ 5    2   0
  Eth 1/ 5    3   0
.
.
.
  Eth 1/ 5   61   0
  Eth 1/ 5   62   0
  Eth 1/ 5   63   0
Console#
```

Port Trunk Configuration

Ports can be combined into an aggregate link to increase the bandwidth of a network connection where bottlenecks exist or to ensure fault recovery. You can create up to six trunks at a time, with any single trunk containing up to four ports.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on

another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than four ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the Web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to six trunks on the switch, with up to four ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

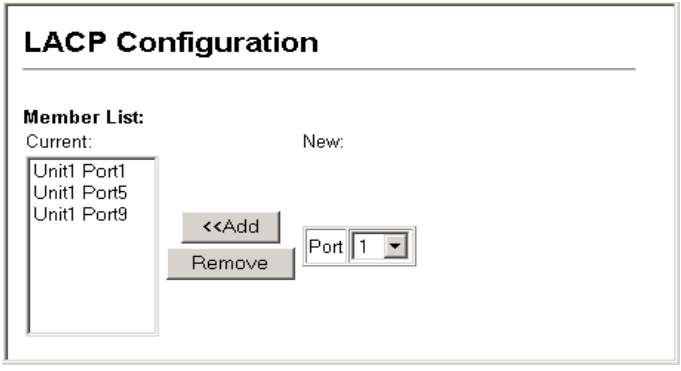
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Dynamically Configuring a Trunk with LACP

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

Web – Click Trunk, LACP Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.



CLI – The following example enables LACP for ports 10 and 11. Just connect these ports to two LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/10                          3-92
Console(config-if)#lacp                                          3-179
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                    3-103
Information of Trunk 1
 Basic information:
  Port type: 1000t
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/10, Eth1/11,
Console#
```

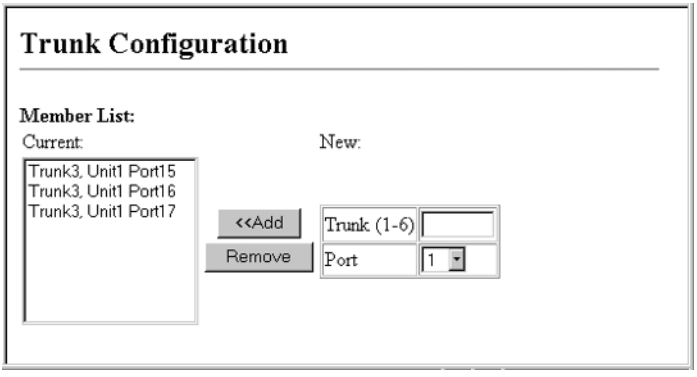
Statically Configuring a Trunk

Command Usage

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. The static trunks on this switch are Cisco EtherChannel compatible.

- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

Web – Click Trunk, Trunk Configuration. Enter a trunk ID of 1-6 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.



CLI – This example creates trunk 1 with ports 11 and 12. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1                          3-92
Console(config-if)#exit
Console(config)#interface ethernet 1/11                           3-92
Console(config-if)#channel-group 1                                3-178
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                     3-103
Information of Trunk 1
 Basic information:
  Port type: 1000t
  Mac address: 22-22-22-22-22-2c
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Created by: User
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12,
Console#
```

Configuring SNMP

The switch includes an onboard agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports, based on the Simple Network Management Protocol (SNMP). A network management station can access this information using management software. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first

submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

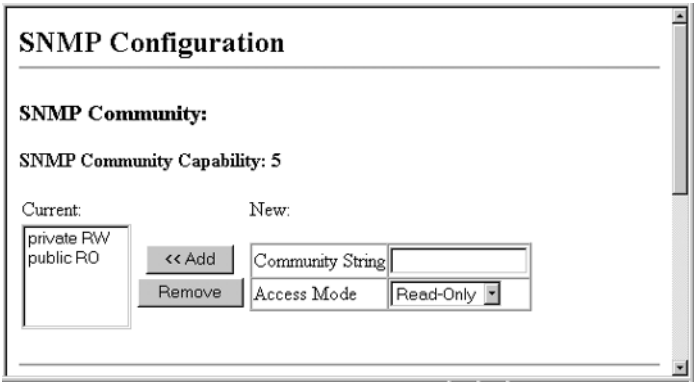
Setting Community Access Strings

You may configure up to five community strings authorized for management access. For security reasons, you should consider removing the default strings.

Command Attributes

- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.
- **Access Mode** – Sets the access rights for a community string:
  - **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, SNMP Configuration. Enter a new string in the Community String box and select the access rights from the Access Mode drop-down list, then click Add.



CLI – The following example adds the string "spiderman" with read/write access.

```
Console(config)#snmp-server community spiderman rw          3-65
Console(config)#
```

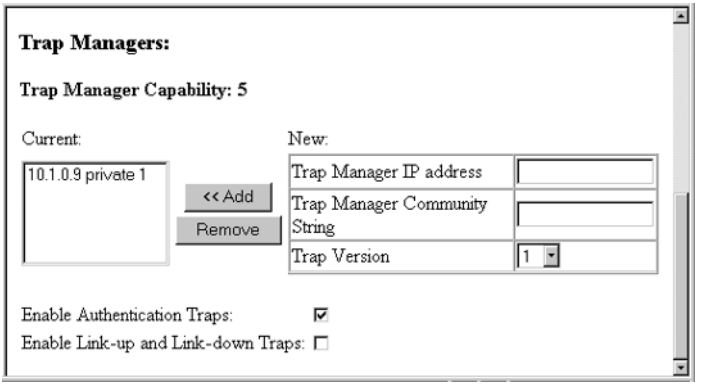
Specifying Trap Managers

You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- If you do not enter a trap manager host IP address, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one host IP address.
- The switch can send SNMP version 1 or version 2c traps to a host IP address, depending on the SNMP version that the management station supports. The default is to send SNMP version 1 traps.
- You can enable or disable authentication messages and link-up-down messages via the Web interface.
- You can enable or disable authentication messages, link-up-down messages, or all notification types via the CLI.

Web – Click SNMP, SNMP Configuration. Fill in the Trap Manager IP Address box and the Trap Manager Community String box, mark Enable Authentication Traps if required, and then click Add.



CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 batman            3-67
Console(config)#snmp-server enable traps authentication       3-69
```

SNMP IP Filtering

The switch allows you to create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.

IP addresses that are permitted SNMP access are specified by an IP address together with a subnet mask that identifies the range of valid addresses. For example:

IP address 192.168.1.1 and mask 255.255.255.0 — Specifies a valid IP address group from 192.168.1.0 to 192.168.1.255.

IP address 192.168.1.1 and mask 255.255.255.255 — Specifies a valid IP address of 192.168.1.1 only.

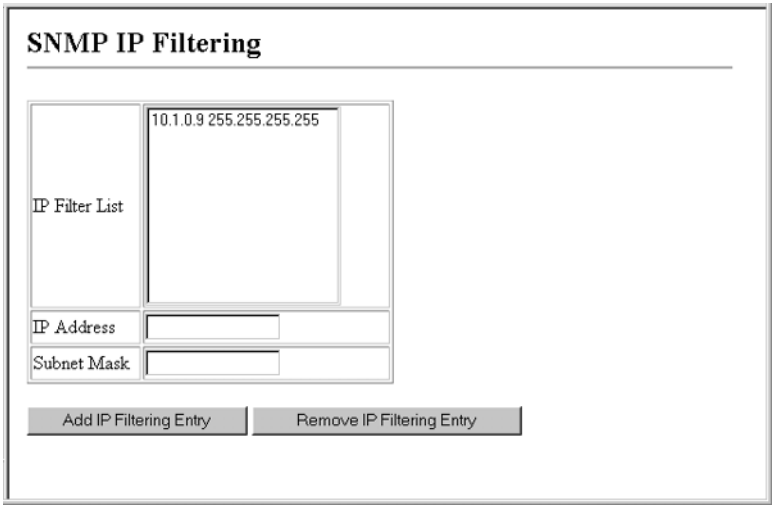
Note: IP filtering does not affect management access to the switch using the Web interface or Telnet.

Command Attributes

- **IP Filter List** — Displays a list of the IP address/subnet mask entries currently configured for SNMP access.
- **IP address** — Specifies a new IP address to add to the **IP Filter List**.
- **Subnet Mask** — Specifies a single IP address or group of addresses. If the IP is the address of a single management station, the mask should be set to 255.255.255.255. Otherwise, the IP address group is specified by the mask.

Note: The default setting is null, which allows all IP groups SNMP access to the switch. If one IP address is configured, the IP filtering is enabled and only addresses in the IP group will have SNMP access.

Web – Click SNMP, SNMP IP Filtering. To add an IP address, type the new IP address in the IP Address box, type the appropriate subnet mask in the Subnet Mask box, and then click "Add IP Filtering Entry." To delete an IP address, click the entry in the IP Filter List, and then click "Remove IP Filtering Entry."



CLI – The following is an example of configuring an SNMP IP filter.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255       3-70
Console(config)#
```

Multicast Configuration

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Configuring IGMP Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly.

- **IGMP Query** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Disabled)

- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Default: 2, Range: 2 - 10)

- **IGMP Query Interval** — Sets the frequency (in seconds) at which the switch sends IGMP host-query messages. (Default: 125, Range: 60 - 125)

- **IGMP Report Delay** — Sets the time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Default: 10, Range: 5 - 30)

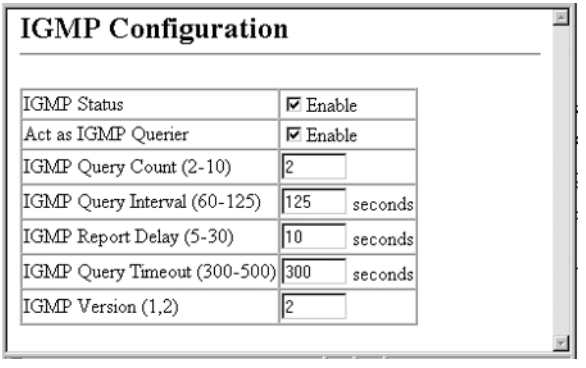
- **Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Default: 300 seconds, Range: 300 - 500)

- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Default: 2, Range: 1 - 2)

Notes: 1. All systems on the subnet must support the same version.

2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)



CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                                  3-149
Console(config)#ip igmp snooping querier                          3-153
Console(config)#ip igmp snooping query-count 10                   3-154
Console(config)#ip igmp snooping query-interval 100               3-155
Console(config)#ip igmp snooping query-max-response-time 20       3-156
Console(config)#ip igmp snooping router-port-expire-time 300      3-157
Console(config)#ip igmp snooping version 2                        3-151
Console(config)#exit
Console#show ip igmp snooping                                     3-152
 Igmp Snooping Configuration
 ---------------------------------------------
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Query time-out          : 300 sec
 IGMP snooping version   : Version 2
Console#
```

Interfaces Attached to a Multicast Router

Multicast routers use the information obtained from IGMP Query, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

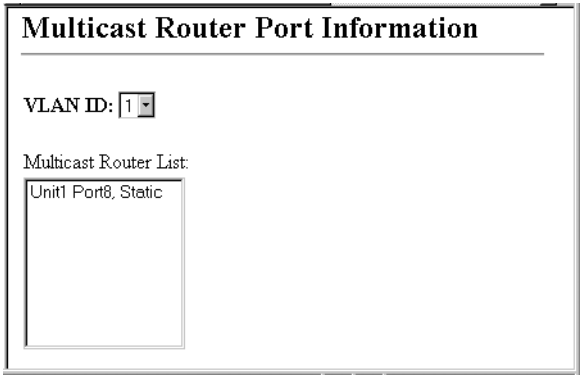
You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Displaying Interfaces Attached to a Multicast Router

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                    3-159
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
```

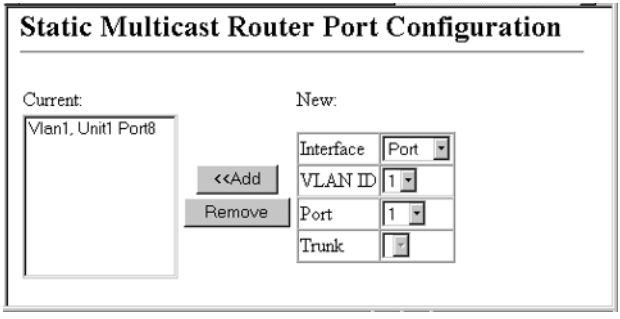
Specifying Interfaces Attached to a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have completed adding interfaces to the list, click Apply.



CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11 3-158
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                  3-159
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11  Static
```

Displaying Port Members of Multicast Services

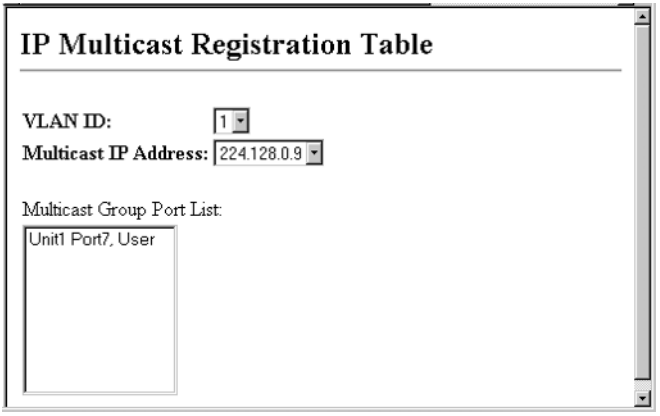
You can display the port members associated with a specified VLAN and multicast IP address.

Command Attribute

- **VLAN ID** – Selects the VLAN in which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service

- **Multicast Group Port List** – Ports propagating a multicast service; i.e., ports that belong to the indicated VLAN group.

Web – Click IGMP, IP Multicast Registration Table. Select the VLAN ID and multicast IP address. The switch will display all the ports that are propagating this multicast service.



CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The type field shows if this entry was learned dynamically or was statically configured.

```
Console#show mac-address-table multicast vlan 1                3-152
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Adding Multicast Addresses to VLANs

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in "Configuring IGMP Parameters" on page 2-113. For certain application that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

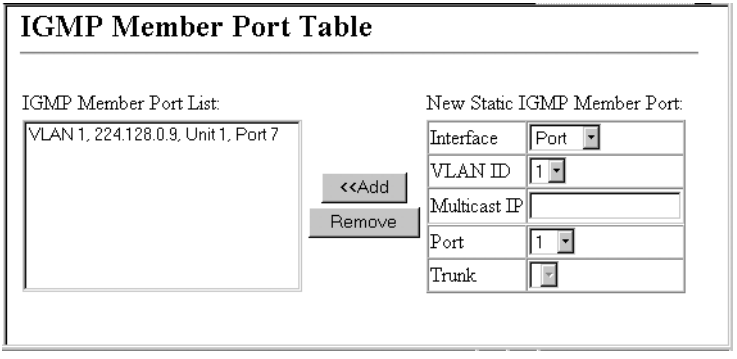
Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and then click Add. After you have completed adding ports to the member list, click Apply.



CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet 1/12                                                    3-150
Console(config)#exit
Console#show mac-address-table multicast vlan 1                  3-152
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Showing Device Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMOM MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through

each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software.

Statistical Values

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcas address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

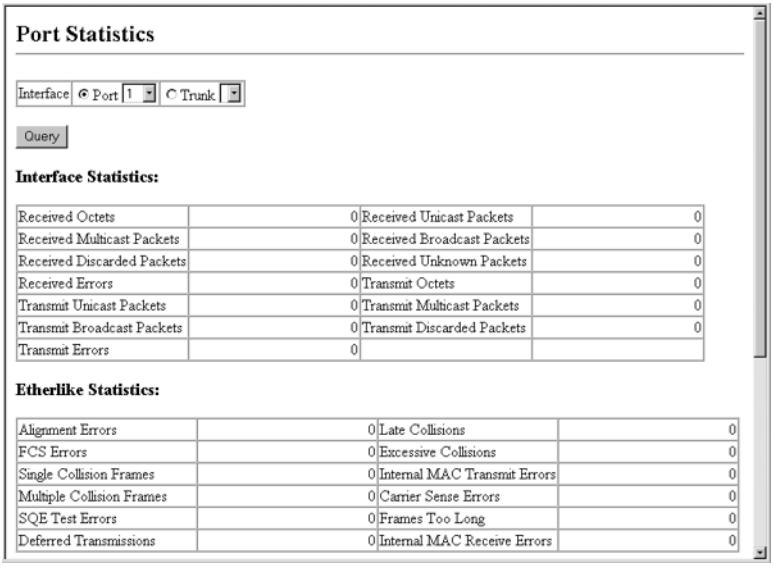
Parameter	Description
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Parameter	Description
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.

Parameter	Description
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

Parameter	Description
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Statistics, Port Statistics. Select the required interface, and then click Query. You can also use the Refresh button at the bottom of the page to update the screen.



Port Statistics

Interface ◉ Port 1 ○ Trunk

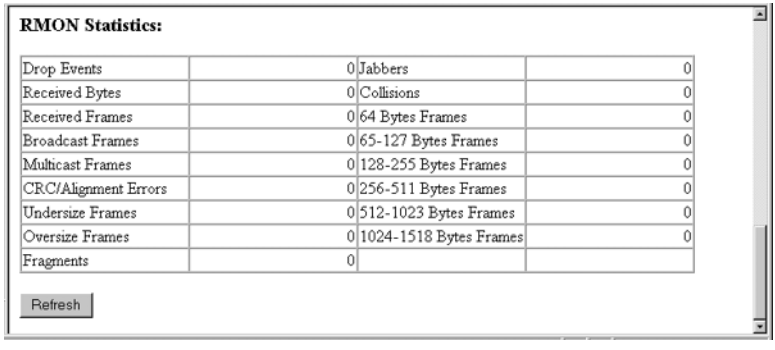
Query

Interface Statistics:

Received Octets	0	Received Unicast Packets	0
Received Multicast Packets	0	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	0
Transmit Unicast Packets	0	Transmit Multicast Packets	0
Transmit Broadcast Packets	0	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0



RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	0	Collisions	0
Received Frames	0	64 Bytes Frames	0
Broadcast Frames	0	65-127 Bytes Frames	0
Multicast Frames	0	128-255 Bytes Frames	0
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

CLI – This example shows statistics for port 13.

```
Console#show interfaces counters ethernet 1/13                    3-104
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets:
1616
Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets:
1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518
octets: 871
Console#
```

801.1X Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first enter a user ID and password for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use a single user ID and password for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LAN (EAPOL) with MD5 authentication to exchange authentication protocol messages with the client, and a remote login authentication server (i.e., RADIUS) to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an identity request. The client provides its identity to the switch, which it forwards to the authentication server. The authentication server verifies the client identity and sends this information back to the switch. The switch then issues an MD5 access challenge to the client, and the client returns an MD5 response to the switch based on its user ID and password. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x "Auto" mode.
- Each client requiring authentication must have 802.1x client software installed and be properly configured. The configuration includes specifying the client identity (user ID)

and the password, as well as selecting MD5 as the authentication method.

- An accessible and functioning RADIUS server.

802.1x Port Configuration

The 802.1x protocol includes parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

The **Switch/802.1x/802.1x Port Configuration** page allows you to enable and configure the 802.1x authentication mode and parameters for each port. The page contains the following editable fields:

- **Mode** — Sets a port's authentication mode to one of the following options:
  - **Auto** – Requires a 802.1x-aware client to be authorized by the authentication server. Clients that are not 802.1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either 802.1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either 802.1x-aware or otherwise.
- **Re-authen** — Sets the client to be re-authenticated after the interval specified by the **Re-authen/Period**. During the re-authentication process of verifying the user ID and password on the RADIUS server, the client remains connected the network. Only if re-authentication fails is the port blocked. Re-authentication can be used to detect if a new device is

plugged into a switch port.
(Default: Disabled)

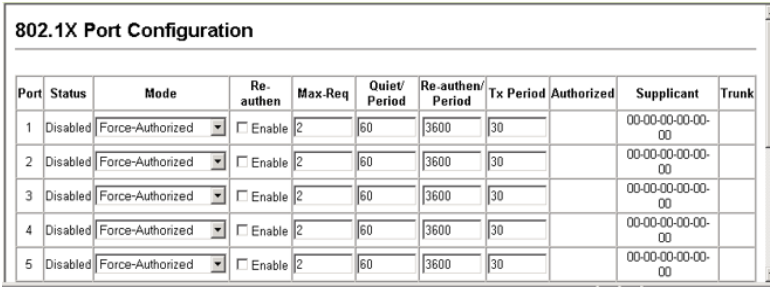
- **Max Req** — Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Quiet/Period** — Sets the time that a switch port waits after the **Max Req** count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Re-authen/Period** — Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **TX Period** — Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet.
(Range: 1-65535; Default: 30 seconds)

The **Switch/802.1x/802.1x Port Configuration** page also displays the following information for each port:

- **Status** — Indicates if authentication is enabled or disabled on the port.
- **Authorized** — Indicates a port's current authentication status:
  - **Yes** – The connected client is authorized.
  - **No** – The connected client is not authorized.
  - [*Blank*] – Displays nothing when 802.1x is disabled on a port.
- **Supplicant** — Indicates the MAC address of a connected client.

- **Trunk** — Indicates if the port is configured as a trunk port.

To save any changes you make in this page, click **Apply Changes**. If you don't want to save the changes, click **Refresh**



802.1X Port Configuration

Port	Status	Mode	Re-authen	Max-Req	Quiet/ Period	Re-authen/ Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
2	Disabled	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	

CLI – This example shows configurable features for port 13.

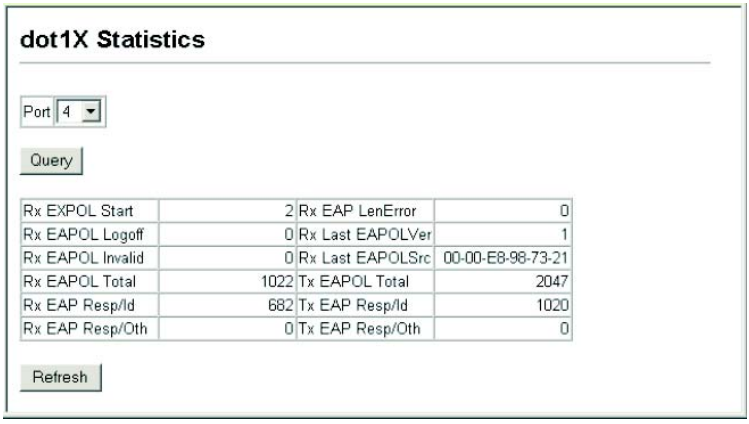
```
Console(config)#interface ethernet 1/13
Console(config-if)#dot1x port-control auto
Console(config-if)#dot1x re-authentication
Console(config-if)#dot1x max-req 10
Console(config-if)#dot1x timeout quiet-period 5
Console(config-if)#dot1x timeout re-authperiod 5
Console(config-if)#dot1x timeout tx-period 1
```

802.1x Statistics

The 802.1x protocol includes statistics for 802.1x protocol exchanges for any port.

Statistical Values

Parameter	Description
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.



dot1X Statistics

Port 4

Query

Rx EXPOL Start	2	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	1
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-E8-98-73-21
Rx EAPOL Total	1022	Tx EAPOL Total	2047
Rx EAP Resp/Id	682	Tx EAP Resp/Id	1020
Rx EAP Resp/Oth	0	Tx EAP Resp/Oth	0

Refresh

CHAPTER 3
COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the SMC8612T is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.

2. At the prompt, enter the user name and system password. The CLI will display the "Vty-0#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-0>" for the guest to show that you are using normal access mode (i.e., Normal Exec).

3. Enter the necessary commands to complete your desired tasks.

4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the SMC8612T is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "configure" example, typing **con** followed by a tab will result in printing the command up to "**configure**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, Interface, Line, or VLAN Database). You can also display a list of valid

keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  bridge-ext         Bridge extend information
  garp               Garp property
  gvrp               Show gvrp information of interface
  history            Information of history
  interfaces         Information of interfaces
  ip                 IP information
  line               TTY line information
  logging            Show the contents of logging buffers
  mac-address-table  Set configuration of the address table
  map                Map priority
  port               Characteristics of the port
  queue              Information of priority queue
  radius-server      Radius server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  spanning-tree      Specify spanning-tree
  ssh                Secure shell
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console>show interfaces ?
  counters    Information of interfaces counters
  status      Information of interfaces status
  switchport  Information of interfaces switchport
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember

not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp           spanning-tree   ssh            startup-config  system
Console#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of

the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode
Exec	Normal
	Privileged
Configuration*	Global
	Interface
	Line
	VLAN

* You must be in Privileged Exec mode to access any of the configuration modes.

Exec Commands

When you open a new console session on switch with the user name "guest," the system enters Normal Exec command mode (or guest mode). Only a limited number of the commands are available in this mode. You can access all the commands only in Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name "admin," or enter the **enable** command (followed by the privileged level password if so configured). The command prompt displays as "Console>" for Normal Exec mode and "Console#" for Privileged Exec mode.

To enter Privileged Exec mode, enter the following commands and passwords:

```
Username: admin
Password: [system login password]

      CLI session with the SMC8612T is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [system login password]

      CLI session with the SMC8612T is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password if so configured]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into three different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port configuration, and include command such as **parity** and **databits**.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter Interface, Line Configuration, or VLAN mode, you must enter the "**interface** ...," "**line**..." or "**vlan database**" command while in Global Configuration mode. The system prompt will change to "Console(config-if)#," "Console(config-line)#" or Console(config-vlan)" indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Privileged Exec mode.

```
Console(config)#interface ethernet 1/5
Console(config-if)#exit
Console(config)#line console
Console(config-line)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?"

character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	**Function**
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-P	Shows the last command.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	3-14
Flash/File	Manages code image or switch configuration files	3-20
System Management	Controls system logs, system passwords, user name, jumbo frame support, browser management options, HTTPS, SSH, and a variety of other system information	3-27
Authentication	Configures RADIUS and TACACS+ client-server authentication for logon access	3-55
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	3-64
IP	Configures the IP address and gateway for management access, displays the default gateway, or pings a specified device	3-73
Line	Sets communication parameters for the serial port, including baud rate and console time-out.	3-80
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	3-91
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time	3-107
Spanning Tree	Configures Spanning Tree settings for the switch	3-113
VLAN	Configures VLAN settings, and defines port membership for VLAN groups	3-130
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	3-141

Command Group	Description	Page
IGMP Snooping	Configures IGMP multicast filtering, querier eligibility, query parameters, and specifies ports attached to a multicast router	3-148
Priority	Sets port priority for untagged frames, relative weight for each priority queue, also sets priority for IP precedence and DSCP	3-160
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	3-174
Port Trunking and LACP	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	3-177

Note that the access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
IC (Interface Configuration)
LC (Line Configuration)
VC (VLAN Database Configuration)

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	3-14
disable	Returns to normal mode from privileged mode	PE	3-15
configure	Activates global configuration mode	PE	3-16
reload	Restarts the system	PE	3-18
end	Returns to Privileged Exec mode	GC, IC, LC, VC	3-18
exit	Returns to the previous configuration mode, or exits the CLI	any	3-19
quit	Exits a CLI session	NE, PE	3-19
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 3-7.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels:
0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- "super" is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 3-31.)
- The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.
- You only need to use Level 15. Setting the password for Level 0 has no effect.
- You cannot set a null password with the **enable password** command. You will have to enter a password to access the Privileged Exec mode.

Example

```
Console#enable
Console#
```

Related Commands

disable (3-15)
enable password (3-31)

disable

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 3-7.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

enable (3-14)

configure

Use this command to activate Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See "Understanding Command Modes" on page 3-7.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (3-18)

show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 20 commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

Use this command to restart the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in nonvolatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

end

Use this command to return to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

quit

Use this command to exit the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

Flash/File Commands

These commands are used to manage system code and configuration files.

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from Flash memory or a TFTP server	PE	3-21
delete	Deletes a file or code image	PE	3-23
dir	Displays a list of files in Flash memory	PE	3-24
whichboot	Displays the files booted	PE	3-25
boot system	Specifies the file or image used to start up the system	GC	3-26

copy

Use this command to move (upload/download) a code image or configuration file between the switch's Flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy *file* {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** | **https-certificate**}

- *file* - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Copies an HTTPS certificate from an TFTP server to the switch.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The file names are case sensitive. The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- The number of user-defined configuration files is limited only by available Flash memory space.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use "Factory_Default_Config.cfg" as the destination.
- To replace the startup configuration, you must use startup-config as the destination.
- The Boot ROM image cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image. See "Upgrading Firmware via the Serial Port" on page B-1 for more details.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
/
Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
/
Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
/
Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

delete

Use this command to delete a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- "Factory_Default_Config.cfg" cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from Flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (3-24)

dir

Use this command to display a list of files in Flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file
- **config** - Switch configuration file
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
                        file name      file type startup size (byte)
-------------------------------- -------------- ------- -----------
                        diag_0060 Boot-Rom image       Y      111360
                        run_01642 Operation Code       N     1074304
                         run_0200 Operation Code       Y     1083008
      Factory_Default_Config.cfg    Config File       N        2574
                          startup    Config File       Y        2710
-----------------------------------------------------------------------
                                          Total free space:         0
Console#
```

whichboot

Use this command to display which files booted.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table on the previous page for a description of the file information displayed by this command.

```
Console#whichboot
        file name      file type startup size (byte)
---------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

boot system

Use this command to specify the file or image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM
- **config** - Configuration file
- **opcode** - Run-time operation code

The colon (:) is required.

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (3-24)
whichboot (3-25)

System Management Commands

These commands are used to control system logs, passwords, user name, browser configuration options, and display or configure a variety of other system information.

Command	Function	Mode	Page
Device Description Command			
hostname	Specifies or modifies the host name for the device	GC	3-29
User Access Commands			
username	Sets user name authentication at login	GC	3-30
enable password	Sets a password to control access to various privilege levels	GC	3-31
Jumbo Frame Command			
jumbo frame	Allows jumbo frames to pass through the switch	GC	3-32
Web Server Commands			
ip http port	Specifies the port to be used by the Web browser interface	GC	3-33

Command	Function	Mode	Page
ip http server	Allows the switch to be monitored or configured from a browser	GC	3-34
ip http secure-server	Enables the HTTPS server on the switch	GC	3-35
ip http secure-port	Specifies the UDP port number used for HTTPS connection to the switch's Web interface	GC	3-36
Secure Shell Commands			
ip ssh server	Enables the SSH server on the switch	GC	3-38
ip ssh	Specifies the authentication timeout for the SSH server and the number of retries allowed by a client	GC	3-37
disconnect ssh	Terminates an SSH connection	PE	3-39
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	3-40
show ssh	Displays the status of current SSH sessions	PE	3-40
Event Logging Commands			
logging on	Controls logging of error messages	GC	3-41
logging history	Limits syslog messages sent to the SNMP network management station based on severity	GC	3-42
logging host	Adds a syslog server host IP address that will receive logging messages	GC	3-44
logging facility	Sets the facility type for remote logging of syslog messages	GC	3-45
logging trap	Limits syslog messages saved to a remote server based on severity	GC	3-45
clear logging	Clears messages from the logging buffer	PE	3-47
show logging	Displays the state of logging	PE	3-47

Command	Function	Mode	Page
System Status Commands			
show startup-config	Displays the contents of the configuration file (stored in Flash memory) that is used to start up the system	PE	3-48
show running-config	Displays the configuration data currently in use	PE	3-51
show system	Displays system information	NE, PE	3-52
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client	NE, PE	3-53
show version	Displays version information for the system	NE, PE	3-54

hostname

Use this command to specify or modify the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname SMC8612T
Console(config)#
```

username

Use this command to require user name authentication at login. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}
no username *name*

- *name* - The name of the user.
  Up to 8 characters, case sensitive.
  Maximum number of users: 16
- **access-level** *level* - Specifies the user level.
- The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

username	access-level	password
guest admin	0 15	guest admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the administrator (Privileged Exec) and guest (Normal Exec) passwords. Remember to record them in a safe place. Use the enable password command to set the password for access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level for which the password applies.
- The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Only level 15 is valid for this command.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.

Default Setting

This default password is "super"

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (3-14)

jumbo frame

Use this command to enable jumbo frames through the switch. Use the **no** form to disable jumbo frames.

Syntax

jumbo frame
no jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9000 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- Enabling jumbo frames will limit the maximum threshold for broadcast storm control to 64 packets per second. (See the "broadcast" command on page 3-100.)

Example

```
Console(config)#jumbo frame
Console(config)#
```

ip http port

Use this command to specify the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (3-34)

ip http server

Use this command to allow this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (3-33)

ip http secure-server

Use this command to enable the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's Web interface. Use the **no** form to disable this function.

Syntax

ip http secure-server
no ip http secure-server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently.
- If you enable HTTPS, you must indicate this in the URL: **https://***device*[*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x.

- The following Web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

* To specify a secure-site certificate, see"Replacing the Default Secure-site Certificate" on page -23. Also refer to the copy command on page 3-21.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (3-36)

ip http secure-port

Use this command to specify the UDP port number used for HTTPS/SSL connection to the switch's Web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:
  https://*device***:***port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (3-35)

ip ssh

Use this command to configure authentication control parameters for the Secure Shell (SSH) server on this switch. Use the **no** form to restore the default settings.

Syntax

ip ssh {[**timeout** *seconds*] | [**authentication-retries** *count*]}
no ip ssh {[**timeout**] | [**authentication-retries**]}

- *seconds* – The timeout for client response during SSH negotiation. (Range: 1-120)
- *count* – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

timeout: 120 seconds
count: 3

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (3-40)

ip ssh server

Use this command to enable the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

ip ssh server
no ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

- The SSH server uses RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

Example

```
Console(config)#ip ssh server
Console(config)#
```

Related Commands

show ssh (3-40)

disconnect ssh

Use this command to terminate a Secure Shell (SSH) client connection.

Syntax

disconnect ssh *connection-id*

connection-id – The session identifier as displayed in the **show ip ssh** command.

Command Mode

Privileged Exec

Example

```
Console#disconnect ssh 0
Console#
```

Related Commands

show ip ssh (3-40)

show ssh

Use this command to display the current Secure Shell (SSH) server connections.

Command Mode

Privileged Exec

Command Usage

This command shows the following information:

- **Session** – The session number. (Range: 0-3)
- **Username** – The user name of the client.
- **Version** – The Secure Shell version number.
- **Encrypt method** – The encryption method. (Options: cipher-des, cipher-3des)
- **Negotiation state** – The authentication negotiation state.

Example

```
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   1.5      cipher-3des   session-started
Console#
```

show ip ssh

Use this command to display the connection settings used when authenticating client access to the Secure Shell (SSH) server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
Information of secure shell
SSH status: enable
SSH authentication timeout: 120
SSH authentication retries: 3
Console#
```

Related Commands

ip ssh (3-37)

logging on

Use this command to control logging of error messages. This command sends debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the **logging history** command to control the type of error messages that are stored in memory. The **logging trap** command controls the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (3-42)
logging trap (3-45)
clear logging (3-47)

logging history

Use this command to limit syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in Flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the level arguments listed below. Messages sent include the selected level up through level 0.

Level Argument	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)	LOG_CRIT

Level Argument	Level	Description	Syslog Definition
errors	3	Error conditions (e.g., invalid input, default used)	LOG_ERR
warnings	4	Warning conditions (e.g., return false, unexpected return)	LOG_WARNING
notifications	5	Normal but significant condition, such as cold start	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for Flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

Use this command to add a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

logging host *host_ip_address*
no logging host *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

Use this command to set the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

logging facility *type*
no logging facility *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

Use this command to limit syslog messages saved to a remote server based on severity. Use the **no** form to return the remote logging of syslog messages to the default level.

Syntax

logging trap *level*
no logging trap *level*

level - One of the level arguments listed below.

Messages sent include the selected level up through level 0.

Level Argument	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)	LOG_CRIT
errors	3	Error conditions (e.g., invalid input, default used)	LOG_ERR
warnings	4	Warning conditions (e.g., return false, unexpected return)	LOG_WARNING
notifications	5	Normal but significant condition, such as cold start	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Default Setting

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear logging

Use this command to clear messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in Flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging (3-47)

show logging

Use this command to display the logging configuration for system and event messages.

Syntax

show logging {**flash** | **ram** | **trap**}

- **flash** - Event history stored in Flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- **trap** - Messages sent to remote syslog servers.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show logging flash
Syslog logging: Disable
History logging in FLASH: level errors
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: enable
REMOTELOG facility type: local use 3
REMOTELOG level type: Warning conditions
REMOTELOG server ip address: 10.1.0.3
REMOTELOG server ip address: 10.1.0.4
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[3] 0:0:41 1/1/1
   "VLAN 1 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[2] 0:0:41 1/1/1
   "STP topology change notification."
   level: 6, module: 6, function: 1, and event no.: 1
[1] 0:0:12 1/1/1
   "Unit 1, Port  5 link-up notification."
   level: 6, module: 6, function: 1, and event no.: 1
[0] 0:0:11 1/1/1
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

show startup-config

Use this command to display the configuration file stored in nonvolatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - IP address configured for VLANs
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1

   .
   .
   .
   .
   .
   .
   .

interface ethernet 1/12
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
line console
!
!
line vty
!
!
end
Console#
```

Related Commands

show running-config (3-51)

show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - IP address configured for VLANs
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro

   .
   .
   .
   .
   .

ip http port
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
no bridge 1 spanning-tree
!
line console
!
line vty
!
end
Console#
```

Related Commands

show startup-config (3-48)

show system

Use this command to display system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to "Displaying System Information" on page 2-8
- The POST results should all display "PASS." If any POST test indicates "FAIL," contact your distributor for assistance.

Example

```
Console#show system
System description: SMC8612T
System OID string: 1.3.6.1.4.1.202.20.25
System information
 System Up time: 0 days, 1 hours, 23 minutes, and 44.61 seconds
 System Name            : SMC8612T switch
 System Location        : Boston
 System Contact         : Charles
 MAC address            : 00-30-f1-47-58-3a
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result            :
UART Loopback Test.....................PASS
Timer Test.............................PASS
DRAM Test .............................PASS
I2C Initialization.....................PASS
Runtime Image Check ...................PASS
PCI Device Check ......................PASS
Switch Driver Initialization...........PASS
Switch Internal Loopback Test..........PASS
------------------ DONE -------------------
Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
 Username accounts:
  Username Privilege
  -------- ---------
     guest          0
     admin         15

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

show version

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See "Displaying System Information" on page 2-8 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit1
 Serial number           :A217056372
 Service tag             :[NONE]
 Hardware version        :R0C
 Number of ports         :12
 Main power status       :up
 Redundant power status :not present
Agent(master)
 Unit id                 :1
 Loader version          :1.0.0.0
 Boot rom version        :1.0.0.2
 Operation code version :1.0.1.3
Console#
```

Authentication Commands

You can configure the switch to authenticate users logging into the system for management access using local or authentication-server methods.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS+-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode	Page
Authentication Method			
authentication login	Defines logon authentication method and precedence	GC	3-56

Command	Function	Mode	Page
RADIUS Client			
radius-server host	Specifies the RADIUS server	GC	3-58
radius-server port	Sets the RADIUS server network port	GC	3-58
radius-server key	Sets the RADIUS encryption key	GC	3-59
radius-server retransmit	Sets the number of retries	GC	3-60
radius-server timeout	Sets the interval between sending authentication requests	GC	3-60
show radius-server	Shows the current RADIUS settings	PE	3-61
TACACS+ Client			
tacacs-server host	Specifies the TACACS+ server	GC	3-61
tacacs-server port	Specifies the TACACS+ server network port	GC	3-62
tacacs-server key	Sets the TACACS+ encryption key	GC	3-63
show tacacs-server	Shows the current TACACS+ settings	GC	3-63

authentication login

Use this command to define the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local authentication.
- **radius** - Use RADIUS server authentication.
- **tacacs** - Use TACACS+ server authentication.

Default Setting

Local only

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS and TACACS+ logon authentication can control management access via the console port, a Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius local
Console(config)#
```

Related Commands

username (3-30) - for setting local user names and passwords

radius-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of a RADIUS server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

radius-server port

Use this command to set the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

Use this command to set the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

Use this command to set the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

Use this command to set the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

Use this command to display the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Server IP address: 10.1.0.99
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

tacacs-server host

Use this command to specify the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

Use this command to specify the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

Use this command to set the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

Use this command to display the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with radius server:
 Server port number: 49
Console#
```

SNMP Commands

Controls access to this switch from SNMP management stations, as well as the error types sent to trap managers.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	3-65
snmp-server contact	Sets the system contact string	GC	3-66
snmp-server location	Sets the system location string	GC	3-66
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	3-67
snmp-server enable traps	Enables the device to send SNMP notifications (i.e., SNMP traps)	GC	3-69
snmp ip filter	Sets IP addresses of clients allowed to management access to the switch via SNMP	GC	3-70
show snmp	Displays the status of SNMP communications	NE, PE	3-71

snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first snmp-server community command you enter enables SNMP (SNMP v1 and v2c). The **no** snmp-server community command disables all versions of SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

Use this command to set the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (3-66)

snmp-server location

Use this command to set the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (3-66)

snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *{host-addr community-string}* [**version 1 | 2c**]
no snmp-server host *host-addr*

- *host-addr* - Name or Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1 or SNMP v2c traps.

Default Setting

Host Address: None
SNMP Version: 1

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- The switch can send SNMP version 1 or version 2c traps to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 traps.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (3-69)

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

snmp-server enable traps [**authentication** | **link-up-down**]
no snmp-server enable traps [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (3-67)

snmp ip filter

Sets the IP addresses of clients that are allowed management access to the switch via SNMP. Use the **no** form of this command to remove an IP address.

Syntax

snmp ip filter *ip_address subnet_mask*
no snmp ip filter *ip_address subnet_mask*

- *ip_address* - An IP address indicating a client or group of clients that are allowed SNMP access to the switch.
- *subnet_mask* - An address bitmask of decimal numbers that represent the address bits to match.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.
- Address bitmasks are similar to a subnet mask, containing four decimal integers from 0 to 255, each separated by a period. The binary mask uses “1” bits to indicate “match” and “0” bits to indicate “ignore.”

- If the IP is the address of a single management station, the bitmask should be set to 255.255.255.255. Otherwise, the IP address group is specified by the bitmask.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one IP address is configured, the IP filtering is enabled and only addresses in the IP group will have SNMP access.
- IP filtering does not affect management access to the switch using the Web interface or Telnet.

Example

The following example enables SNMP IP filtering on the switch and allows SNMP management access to client IP 10.1.2.3, and client IP group 10.1.3.0 to 10.1.3.255.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#snmp ip filter 10.1.3.0 255.255.255.0
Console(config)#
```

Related Commands

show snmp (3-71)

show snmp

Use this command to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
   0 Trap PDUs

SNMP logging: disabled
SNMP ip filter group:
    1. IP:10.1.2.3 Mask:255.255.255.255 valid
    2. IP:10.1.3.0 Mask:255.255.255.0 valid
Console#
```

IP Commands

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch. If you wish to manually configure IP settings, you need to change the switch's user-specified defaults (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

Command	Function	Mode	Page
ip address	Sets the IP address for this device	IC	3-74
ip dhcp restart	Submits a BOOTP or DCHP client request	PE	3-75
ip default-gateway	Defines the default gateway through which an in-band management station can reach this device	GC	3-76
show ip interface	Displays the IP settings for this device	PE	3-77
show ip redirects	Displays the default gateway configured for this device	PE	3-78
ping	Sends ICMP echo request packets to another node on the network	NE, PE	3-78

ip address

Use this command to set the IP address for this device. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

IP address: 0.0.0.0
Netmask: 255.0.0.0

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers,
  0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).

- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart** command, or by rebooting the switch.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart (3-75)

ip dhcp restart

Use this command to submit a BOOTP or DCHP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- DHCP requires the server to reassign the client's last address if available.

- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address (3-74)

ip default-gateway

Use this command to a establish a static route between this device and management stations that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

Related Commands

show ip redirects (3-78)

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Command Usage

This switch can only be assigned one IP address. This address is used for managing the switch.

Example

```
Console#show ip interface
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects (3-78)

show ip redirects

Use this command to show the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (3-76)

ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, Default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, Default: 32)
  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the ping command:
  - *Normal response* -The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (3-92)

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or a virtual terminal. Note that Telnet is considered a virtual terminal connection, and the only commands that apply to Telnet include **exec-timeout** and **password-thresh**.

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	3-81
login	Enables password checking at login	LC	3-82
password	Specifies a password on a line	LC	3-83
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	3-84
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	3-85
silent-time	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	3-86
databits	Sets the number of data bits per character that are interpreted and generated by hardware	LC	3-87
parity	Defines the generation of a parity bit	LC	3-88
speed	Sets the terminal baud rate	LC	3-89
stopbits	Sets the number of the stop bits transmitted per byte	LC	3-90
show line	Displays a terminal line's parameters	NE, PE	3-90

line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as "Vty" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (3-90)
show users (3-53)

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the password line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the username command (i.e., Default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (3-30)
password (3-83)

password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive).

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatiblity with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (3-82)
password-thresh (3-85)

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to remove the timeout definition.

Syntax

exec-timeout *seconds*
no exec-timeout

seconds - Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If input is detected, the system resumes the current connection; or if no connections exist, it returns the terminal to the idle state and disconnects the incoming session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

Use this command to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *threshold*
no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent-time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (3-86)

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time *seconds*
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Command Usage

If the password threshold was not set with the **password-thresh** command, silent-time begins after the default value of three failed logon attempts.

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (3-85)

databits

Use this command to set the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (3-88)

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

Use this command to set the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 57600, 38400, 19200, 115200 bps)

Default Setting

9600 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

Use this command to set the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

show line

Use this command to display the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
Console#
```

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	3-92
description	Adds a description to an interface configuration	IC	3-93
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	3-94
negotiation	Enables autonegotiation of a given interface	IC	3-95

Command	Function	Mode	Page
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	3-96
flowcontrol	Enables flow control on a given interface	IC	3-97
shutdown	Disables an interface	IC	3-99
switchport broadcast	Configures broadcast storm control	IC	3-100
port security	Enables port security on an interface.	IC	3-101
clear counters	Clears statistics on an interface	PE	3-102
show interfaces status	Displays status for the specified interface	NE, PE	3-103
show interfaces counters	Displays statistics for the specified interface	NE, PE	3-104
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-106

interface

Use this command to configure an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify the Ethernet port, enter the following command:

```
Console(config)#interface ethernet 1/25
Console(config-if)#
```

description

Use this command to add a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to Ethernet port 15.

```
Console(config)#interface ethernet 1/15
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

Use this command to configure the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the **capabilities** list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-95)
capabilities (3-96)

negotiation

Use this command to enable autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

negotiation
no negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (3-96)
speed-duplex (3-94)

capabilities

Use this command to advertise the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

no port-capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch ASIC only supports symmetric pause frames.)

Default Setting

- 100BASE-TX: 10half, 10full, 100half, 100full
- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

flowcontrol

Use this command to enable flow control. Use the **no** form to disable flow control.

Syntax

flowcontrol
no flowcontrol

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** comm and), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.
- Due to a hardware limitation, flow control only works on those ports located in the same chip (ports 1-12 and ports 13-24). Cross-chip flow control does not work.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

capabilities (3-96) (flowcontrol (3-97), symmetric)

shutdown

Use this command to disable an interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second. (Range: 16, 64, 128, 256)

Default Setting

Enabled for all ports
Packet-rate limit: 256 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.
- Enabling jumbo frames for the switch will limit the maximum threshold for broadcast storm control to 64 packets per second.

Example

The following shows how to configure broadcast storm control at 64 packets per second on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#
```

port security

Use this command to enable and configure port security on a port. Use the **no** form to disable port security or reset the intrusion action to the default.

Syntax

port security [**action trap-and-shutdown**]
no port security [**action**]

action - Indicates the security action to be taken when a port security violation is detected (applies globally to all ports).

trap-and-shutdown - Issue an SNMP trap message and disable the port.

Default Setting

Status: Disabled
Action: None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch will stop dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.
- To add new VLAN members at a later time, you can manually add secure addresses with the **mac-address-table static** command, or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.
- If a port is disabled due to a security violation, it must be manually re-enabled by using the **no shutdown** command.
- Although the **port security action** command is an Interface Configuration command, it applies globally to all switch ports.

Example

This example sets the port security action for the switch and enables port security for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown
Console(config-if)#port security
Console(config-if)#
```

clear counters

Use this command to clear statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

Use this command to display the status for an interface.

Syntax

show interfaces status *interface*

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- If no interface is specified, information on all interfaces is displayed.
- For a description of the items displayed by this command, see "Displaying Connection Status" on page 2-36.

Example

```
Console#show interface status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type: 1000T
  Mac address: 00-00-11-11-22-27
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

show interfaces counters

Use this command to display statistics for an interface.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- If no interface is specified, information on all interfaces is displayed.
- For a description of the items displayed by this command, see "Showing Device Statistics" on page 2-122.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/ 7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

Use this command to display the administrative and operational status of the specified interfaces..

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. The items displayed by this command include:

- **Broadcast threshold** – Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 3-100).
- **Lacp status** – Shows if Link Aggregation Control Protocol has been enabled or disabled (page 3-179).
- **VLAN membership mode** – Indicates membership mode as Trunk or Hybrid (page 3-134).
- **Ingress rule** – Shows if ingress filtering is enabled or disabled (page 3-136).
- **Acceptable frame type** – Shows if acceptable VLAN frames include all types or tagged frames only (page 3-135).
- **Native VLAN** – Indicates the default Port VLAN ID (page 3-137).

- **Priority for untagged traffic** – Indicates the default priority for untagged frames (page 3-160).
- **Gvrp status** – Shows if GARP VLAN Registration Protocol is enabled or disabled (page 3-142).
- **Allowed Vlan** – Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 3-138).
- **Forbidden Vlan** – Shows the VLANs this interface can not dynamically join via GVRP (page 3-139).

Example

This example shows the configuration setting for Ethernet port 15.

```
Console#show interfaces switchport ethernet 1/15
Information of Eth 1/15
broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Enabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	3-108
show mac-address-table	Displays entries in the forwarding database	PE	3-109

Command	Function	Mode	Page
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	3-111
mac-address-table aging-time	Sets the aging time of the address table	GC	3-111
show mac-address-table aging-time	Showsthe aging time for the address table	PE	3-112

mac-address-table static

Use this command to map a static address to a port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- *action* -
  - **delete-on-reset** - Assignment lasts until switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
  1/1 vlan 1 delete-on-reset
Console(config)#
```

show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - dynamic address entries
  - Permanent - static entry
  - Delete-on-reset - static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

mac-address-table aging-time

Use this command to set the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Time is number of seconds (17-2184).

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

Use this command to show the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Protocol (STP) for the overall switch, and commands that configure STP for the selected interface.

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	3-114
spanning-tree mode	Configures STP or RSTP mode	GC	3-115
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	3-116
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	3-117
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	3-118
spanning-tree priority	Configures the spanning tree bridge priority	GC	3-119
spanning-tree path-cost method	Configures the path cost method for RSTP	GC	3-120
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC	3-121
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	3-122
spanning-tree port priority	Configures the spanning tree priority of an interface	IC	3-123
spanning-tree portfast	Sets an interface to fast forwarding	IC	3-124
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	3-125
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	3-126

Command	Function	Mode	Page
spanning-tree link-type	Configures the link type for RSTP	IC	3-127
show spanning-tree	Shows the Spanning Tree configuration	PE	3-128

spanning-tree

Use this command to enable the Spanning Tree Protocol globally for this switch. Use the **no** form to disable it.

Syntax

spanning-tree
no spanning-tree

Default Setting

Spanning Tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

The following example enables the Spanning Tree Protocol for this switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

Use this command to select the Spanning Tree mode for this switch. Use the **no** form to disable it.

Syntax

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.
- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

Use this command to configure the SpanningTree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds - Time in seconds. (Range: 4-30 seconds) The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

Use this command to configure the Spanning Tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds)
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

Use this command to configure the Spanning Tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

Use this command to configure the Spanning Tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge.
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

Use this command to configure the path cost method used for the Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

short method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 3-122) takes precedence over port priority (page 3-123).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

Use this command to configure the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limit the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree cost

Use this command to configure the Spanning Tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the interface.
(Range – 1-200,000,000)
The recommended range is -
- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning-Tree Protocol to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Path cost takes precedence over interface priority.
- When the Spanning-Tree pathcost method is set to **short**, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

Related Commands

spanning-tree port-priority (3-123)

spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for an interface. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the Spanning Tree Protocol. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the Spanning Tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree cost (3-122)

spanning-tree portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

spanning-tree portfast
no spanning-tree portfast

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast Spanning Tree mode for the selected interface. In this mode, interfaces skip the Learning state and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STP related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)

- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (3-125)

spanning-tree edge-port

Use this command to specify an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port
no spanning-tree edge-port

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the Spanning Tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not

cause the Spanning Tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

- This command has the same effect as the **spanning-tree portfast** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (3-124)

spanning-tree protocol-migration

Use this command to re-check the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port-number*
  - *unit* - This is device 1.
  - *port-number*
- **port-channel** *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced

STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

spanning-tree link-type

Use this command to configure the link type for the Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.

- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

show spanning-tree

Use this command to show the configuration for the Spanning Tree.

Syntax

show spanning-tree [*interface*]

- *interface*
  - **ethernet** *unit/port-number*
    - *unit* - This is device 1.
    - *port-number*
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the Spanning Tree configuration for the Spanning Tree and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the Spanning Tree configuration for an interface within the Spanning Tree

- For a description of the items displayed under "Spanning-tree information," see "STP Configuration" on page 2-57. For a description of the items displayed for specific interfaces, see "STP Port and Trunk Information" on page 2-61.

Example

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.000011112222
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :1
 Last topology changes time (sec.):25067
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.1
 Designated root      : 32768.000011112222
 Designated bridge    : 32768.000011112222
 Fast forwarding      : disable
 Forward transitions  : 0
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
.
.
.
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Command	Function	Mode	Page
Edit VLAN Groups			
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	3-131
vlan	Configures a VLAN, including VID, name and state	VC	3-132
Configure VLAN Interfaces			
interface vlan	Enters interface configuration mode for specified VLAN	IC	3-133
switchport mode	Configures VLAN membership mode for an interface	IC	3-134
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	3-135
switchport ingress-filtering	Enables ingress filtering on an interface	IC	3-136
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	3-137
switchport allowed vlan	Configures the VLANs associated with an interface	IC	3-138
switchport gvrp	Enables GVRP for an interface	IC	3-142
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-139

Command	Function	Mode	Page
Display VLAN Information			
show vlan	Shows VLAN information	NE, PE	3-140
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	3-103
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-106

vlan database

Use this command to enter VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (3-140)

vlan

Use this command to configure a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
  - **state** - Keyword to be followed by the VLAN state.
    - **active** - VLAN is operational.
    - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- When **no vlan** *vlan-id* is used, the VLAN is deleted.
- When **no vlan** *vlan-id* **name** is used, the VLAN name is removed.
- When **no vlan** *vlan-id* **state** is used, the VLAN returns to the default state (i.e., active).

- VLAN 1 cannot be suspended, but any other VLAN can be suspended.
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using vlan-id 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (3-140)

interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

show vlan (3-140)

switchport mode

Use this command to configure the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types

switchport acceptable-frame-types

Use this command to configure the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port passes all frames, tagged or untagged.
- **tagged** - The port only passes tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic passed on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (3-134)

switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

Use this command to configure the PVID (i.e., Default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

Use this command to configure VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094)

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If switchport mode is set to **trunk**, then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/ untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

Use this command to configure forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.

- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094)

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

show vlan

Use this command to show VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ---------------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12
Console#
```

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Command	Function	Mode	Page
Interface Commands			
switchport gvrp	Enables GVRP for an interface	IC	3-142
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-139
show gvrp configuration	Displays GVRP configuration for selected interface	NE, PE	3-143
garp timer	Sets the GARP timer for the selected function	IC	3-144

Command	Function	Mode	Page
show garp timer	Shows the GARP timer for the selected function	NE, PE	3-145
Global Commands			
bridge-ext gvrp	Enables GVRP globally for the switch	GC	3-146
show bridge-ext	Shows bridge extension configuration	PE	3-147

switchport gvrp

Use this command to enable GVRP for a port. Use the **no** form to disable it.

Syntax

switchport gvrp
no switchport gvrp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

Use this command to show if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Disabled
Console#
```

garp timer

Use this command to set the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  leave >= (2 x join)
  leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP will not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (3-145)

show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds

Console#
```

Related Commands

garp timer (3-144)

bridge-ext gvrp

Use this command to enable GVRP. Use the **no** form to disable it.

Syntax

bridge-ext gvrp
no bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Displaying Basic VLAN Information" on page 2-74 and "Displaying Bridge Extension Capabilities" on page 2-31 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

IGMP Snooping Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Command	Function	Mode	Page
Basic IGMP Commands			
ip igmp snooping	Enables IGMP snooping	GC	3-149
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	3-150
ip igmp snooping version	Configures the IGMP version for snooping	GC	3-151
show ip igmp snooping	Shows the IGMP snooping configuration	PE	3-152
show bridge multicast	Shows the IGMP snooping MAC multicast list	PE	3-152
show ip igmp snooping	Shows the IGMP snooping configuration	PE	3-152
IGMP Querier Commands			
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	3-153
ip igmp snooping query-count	Configures the query count	GC	3-154
ip igmp snooping query-interval	Configures the query interval	GC	3-155
ip igmp snooping query-max-response-time	Configures the report delay	GC	3-156
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	3-157

Command	Function	Mode	Page
Mulitcast Router Commands			
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	3-158
show ip igmp snooping mrouter	Shows multicast router ports	PE	3-159

ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

ip igmp snooping
no ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

Use this command to add a port to a multicast group. Use the no form to remove the port.

Syntax

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan vlan-id static *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet
1/5
Console(config)#
```

ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp router-port-expire-time**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Configuring IGMP Parameters" on page 2-113 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Query time-out: 300 sec
 IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

Use this command to show known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

ip igmp snooping querier

Use this command to enable the switch as an IGMP snooping querier. Use the **no** form to disable it.

Syntax

ip igmp snooping querier
no ip igmp snooping querier

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

Use this command to configure the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

ip igmp snooping query-interval

Use this command to configure the snooping query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

Use this command to configure the snooping report delay. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (3-151)

ip igmp snooping router-port-expire-time

Use this command to configure the snooping query timeout. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must be using IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping query-time-out 300
Console(config)#
```

Related Commands

ip igmp snooping version (3-151)

ip igmp snooping vlan mrouter

Use this command to statically configure a multicast router port. Use the **no** form to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter** *interface*
no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

Use this command to display information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the port in VLAN 1 that is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------ -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command	Function	Mode	Page
Layer 2 Priority Commands			
switchport priority default	Sets a port priority for incoming untagged frames	IC	3-161
queue bandwidth	Assigns round-robin weights to the priority queues	GC	3-162
queue cos map	Assigns class of service values to the priority queues	IC	3-163
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	3-165
show queue cos-map	Shows the class of service map	PE	3-166
show interfaces switchport	Displays the administrative and operational status of an interface	PE	3-106
Layer 3 and 4 Priority Commands			
map ip precedence	Enables IP precedence class of service mapping	GC	3-166
map ip precedence	Maps IP precedence value to a class of service	IC	3-167
map ip dscp	Enables IP DSCP class of service mapping	GC	3-169
map ip dscp	Maps IP DSCP value to a class of service	IC	3-170

Command	Function	Mode	Page
show map ip precedence	Shows the IP precedence map	PE	3-171
show map ip dscp	Shows the IP DSCP map	PE	3-172

switchport priority default

Use this command to set a priority for incoming untagged frames, or the priority of frames received by the device connected to the specified interface. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- This switch provides four priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

Use this command to assign Weighted Round-Robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 255)

Default Setting

Weights 16, 64, 128 and 240 are assigned to queue 0, 1, 2 and 3 respectively.

Command Mode

Global Configuration

Command Usage

WRR allows bandwidth sharing at the egress port by defining scheduling weights.

Example

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the CoS priority queues 0, 1, 2 and 3:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

show queue bandwidth (3-165)

queue cos-map

Use this command to assign class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 3). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The queue ID of the CoS priority queue.
  - Ranges are 0 to 3, where 3 is the highest CoS priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

	Queue			
	1	**2**	**3**	**4**
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Example

The following example shows how to map CoS values 0, 1 and 2 to CoS priority queue 0, value 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Related Commands

show queue cos-map (3-166)

show queue bandwidth

Use this command to display the Weighted Round-Robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

show queue cos-map

Use this command to show the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/11
Information of Eth 1/11
 Queue ID Traffic class
 -------- -------------
    0     1 2
    1     0 3
    2     4 5
    3     6 7
Console#
```

map ip precedence (Global Configuration)

Use this command to enable IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

map ip precedence
no map ip precedence

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

Use this command to set IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping.

IP Precedence Value	CoS Value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

Use this command to enable IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

map ip dscp
no map ip dscp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

Use this command to set IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults.
- This command sets the DSCP Priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip precedence

Use this command to show the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (3-166)
map ip precedence (Interface Configuration) (3-167)

show map ip dscp

Use this command to show the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (3-169)
map ip dscp (Interface Configuration) (3-170)

Mirror Port Commands

This section describes how to configure port mirror sessions.

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	3-174
show port monitor	Shows the configuration for a mirror port	PE	3-175

port monitor

Use this command to configure a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface*
  - **ethernet** *unit/port* (source port)
    - *unit* - Switch (unit 1).
    - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The source and destination port speeds should match, otherwise traffic may be dropped from the source port.
- You can create only one port mirror session.
- The source and destination ports have to be either both in the port range 1-12 or both in the port range 13-24.

Example

The following example configures the switch to mirror all packets from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

Related Commands

show port monitor (3-175)

show port monitor

Use this command to display mirror information.

Syntax

show port monitor [*interface*]

interface

- **ethernet** *unit/port* (source port)
  - *unit* - Switch (unit 1).
  - *port* - Port number.

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Related Commands

port monitor (3-174)

Port Trunking Commands

Ports can be statically grouped into an aggregate link to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP), also known as 802.1ad, to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to be compatible with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	3-92
channel-group	Adds a port to a trunk	IC	3-178
Dynamic Configuration Command			
lacp	Configures LACP for the current interface	IC	3-179
Trunk Status Display Command			
show interfaces status port-channel	Shows trunk information	NE, PE	3-103

Guidelines for Creating Trunks

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can contain up to four 10/100 Mbps ports or up to two 1000 Mbps ports.
- The ports at both ends of a connection must be configured as trunk ports.

- All ports in a trunk must consist of the same media type (i.e., twisted-pair or fiber).
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

channel-group

Use this command to add a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-6)

Default Setting

A new trunk contains no ports.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

- The maximum number of ports that can be combined as a static trunk is four 10/100 Mbps ports, and two 1000 Mbps ports.
- All links in a trunk must operate at the same data rate and duplex mode.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

Use this command to enable 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

lacp
no lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.

- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 10-11. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk 1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/9
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 00-00-11-11-22-2C
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control: Disabled
  Port security: Disabled
  Port security action: None
 Current status:
  Created by: lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/9, Eth1/10, Eth1/11,
Console#
```

APPENDIX A
TROUBLESHOOTING

Troubleshooting Chart

Troubleshooting Chart	
Symptom	**Action**
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure to have configured the agent with a valid IP address, subnet mask and default gateway. • Be sure that your management station has management VLAN access to the switch (default is VLAN 1). • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time.

Troubleshooting Chart	
Symptom	**Action**
Cannot access the on-board configuration program via a serial port connection	• Be sure to have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps. • Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.
Forgot or lost the password	• Set the switch to its default configuration. Make a direct connection to the switch's console port and power cycle the switch. Immediately after powering on, press <Ctrl><u> to access the system file menu. Select <D> to delete all user-defined configuration files. Press <Q> to boot the switch.

APPENDIX B
UPGRADING FIRMWARE VIA THE SERIAL PORT

The switch contains three firmware components that can be upgraded; the diagnostics (or Boot-ROM) code, runtime operation code, and the loader code. The runtime code can be upgraded via the switch's RS-232 serial console port, via a network connection to a TFTP server, or using SNMP management software. The diagnostics and loader code can be upgraded only via the switch's RS-232 serial console port.

Note: You can use the switch's web interface to download runtime code via TFTP. Downloading large runtime code files via TFTP is normally much faster than downloading via the switch's serial port.

You can upgrade switch firmware by connecting a PC directly to the serial Console port on the switch's front panel and using VT100 terminal emulation software that supports the XModem protocol. (See "Required Connections" on page 1-3.)

1. Connect a PC to the switch's Console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.

2. Configure the terminal emulation software's communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to *none*.

3. Power cycle the switch.

4. When the switch initialization screen appears, enter firmware-download mode by pressing <Ctrl><u> immediately after power on. Screen text similar to that shown below displays:

```
File Name                         S/Up Type Size       Create Time
--------------------------------- ---- ---- ---------- -----------
$certificate                        0    7      20480  00:38:34
$logfile_1                          0    3         64  00:00:02
Factory_Default_Config.cfg          0    5       2574  00:00:12
diag_1000                           1    1     116228  00:00:00
r_20019                             1    2    1536972  00:00:01
set-ip.cfg                          1    5       2690  00:40:44
--------------------------------- ---- ---- ---------- ----------
[X]modem Download  [D]elete File  [S]et Startup File
[C]hange Baudrate  [Q]uit
Select>
```

5. Press <C> to change the baud rate of the switch's serial connection.

6. Press <B> to select the option for 115200 baud.

   There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files.

7. Set your PC's terminal emulation software to match the 115200 baud rate. Press <Enter> to reset communications with the switch.

```
Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200
```

8. Check that the switch has sufficient flash memory space for the new code file before starting the download.

You can store a maximum of only two runtime and two diagnostic code files in the switch's flash memory. Use the **[D]elete File** command to remove a runtime or diagnostic file.

9. Press <X> to start to download the new code file.

   If using Windows HyperTerminal, click the "Transfer" button, and then click "Send File...." Select the XModem Protocol and then use the "Browse" button to select the required firmware code file from your PC system. The "Xmodem file send" window displays the progress of the download procedure.

   Note: The download file must be a SMC8612T binary software file from SMC.

10. After the file has been downloaded, you are prompted with "Update Image File:" to specify the type of code file. Press <R> for runtime code, <D> for diagnostic code, or ,<L> for loader code.

    Caution: If you select <L> for loader code, be sure the file is a valid loader code file for the switch. If you download an invalid file, the switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files.

11. Specify a name for the downloaded code file. File names are case-sensitive, should be from 1 to 31 characters, not contain slashes (\ or /), and the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

For example, the following screen text shows the download procedure for a runtime code file:

```
Select>
Xmodem Receiving Start ::
Image downloaded to buffer.


        [R]untime
        [D]iagnostic
        [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Diagnostic Image Filename : r_20019
Updating file system.
File system updated.
[Press any key to continue]
```

12. To set the new downloaded file as the startup file, use the **[S]et Startup File** menu option.

13. When you have finished downloading code files, use the **[C]hange Baudrate** menu option to change the baud rate of the switch's serial connection back to 9600 baud.

14. Set your PC's terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.

15. Press <Q> to quit the firmware-download mode and boot the switch.

GLOSSARY

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 UTP cable.

1000BASE-T

IEEE 802.3ab specification for Gigabit Ethernet over two pairs of Category 5, 5e, or 6 100-ohm UTP cable.

1000BASE-X

IEEE 802.3 shorthand term for any 1000 Mbps Gigabit Ethernet based on 8B/10B signaling.

Auto-negotiation

Signalling method allowing each node to select its optimum operational mode (e.g., 10, 100, or 1000 Mbps and half or full duplex) based on the capabilities of the node to which it is connected.

Bandwidth

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

BOOTP

Boot protocol used to load the operating system for devices connected to the network.

Collision

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

Collision Domain

Single CSMA/CD LAN segment.

CSMA/CD

Carrier Sense Multiple Access/Collision Detect is the communication method employed by Ethernet and Fast Ethernet.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

End Station

A workstation, server, or other device that does not act as a network interconnection.

Ethernet

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

Fast Ethernet

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex

Transmission method that allows switch and network card to transmit and receive concurrently, effectively doubling the bandwidth of that link.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard.

Gigabit Ethernet

A 1000 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Group Attribute Registration Protocol

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX and 100BASE-FX Fast Ethernet.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IEEE 802.3z

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

Internet Control Message Protocol (ICMP)

Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the "querier" and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Media Access Control (MAC)

A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

INDEX

Numerics

802.1x
  configure 2-131, 2-134

A

address table 2-47

B

BOOTP 2-13
broadcast storm, threshold 2-41

C

Class of Service
  configuring 2-87
  queue mapping 2-87
community string 2-107
configuration settings, saving or
    restoring 2-28

D

default priority, ingress port 2-87
default settings 1-14
DHCP 2-13
downloading software 2-26
dynamic addresses, displaying 3-109

E

edge port, STP 3-125

F

firmware version, displaying 2-34
firmware, upgrading 2-26

H

hardware version, displaying 2-34
HTTP, secure server 3-35
HTTPS 3-35

I

IEEE 802.1D 3-115
IEEE 802.1w 3-115
IGMP, configuring 2-113
ingress filtering 2-84
IP address
  BOOTP/DHCP service 2-13
  setting 2-11

L

link type, STP 3-127
log-in
  CLI 3-1
  Web interface 2-2
logon authentication
  RADIUS server 2-16
  TACACS server 2-16

M

main menu 2-5
mirror port, configuring 2-42
multicast
  configuring 2-113
  router 2-117, 3-158

P

passwords
  administrator setting 2-14
path cost, method 3-120
path cost, STP 3-120, 3-122
port priority
  configuring 2-87
  default ingress 2-87
port security, configuring 2-44
ports, configuring 2-36
priority, default port ingress 2-87
priority, STP 3-119
problems, troubleshooting A-1
protocol migration 3-126

R

RADIUS 2-16, 3-55
RADIUS, logon authentication 2-16
RSTP, global configuration 3-115

S

secure hypertext transfer protocol *See* HTTPS
Secure Socket Layer *See* SSL
serial port
  configuring 3-80
SNMP
  community string 2-107
  enabling traps 2-109
  trap manager 2-109
software downloads 2-26
software version, displaying 2-34
Spanning Tree Protocol 2-51
SSL 3-35
startup files
  displaying 2-26
  setting 2-26
statistics, switch 2-122
STP 3-113, 3-114, 3-115
  configuring interfaces 3-113
  edge port 3-125
  interface settings 3-128
  link type 3-127
  priority 3-123
  protocol migration 3-126
system software, downloading from server 2-26

T

TACACS 2-16, 3-55
TACACS, logon authentication 2-16
trap manager 2-109
troubleshooting A-1
trunk
  configuration 2-100
  LACP 2-102
  static 2-104

U

upgrading software 2-26
user password 2-14

V

VLANs
  configuring 2-70

W

Web interface
  access requirements 2-1
  configuration buttons 2-3
  home page 2-3
  menu list 2-5
  panel display 2-4

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe (8:00 AM - 5:30 PM UK Time)
44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
support@smc-asia.com
Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
World Wide Web:
http://www.smc.com
http://www.smc-europe.com
http://www.smc-asia.com

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-93-477-4935;	Fax 34-93-477-3774
UK:	44 (0) 118 974 8700;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 02 739 12 33;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Switzerland:	41 (0) 1 9409971;	Fax 41 (0) 1 9409972
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Northern Europe:	44 (0) 118 974 8700;	Fax 44 (0) 118 974 8701
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	27-11 314 1133;	Fax 27-11 314 9133
North Africa:	34 93 477 4920;	Fax 34 93 477 3774
Russia:	7 (095) 290 29 96;	Fax 7 (095) 290 29 96
PRC:	86-21-6485-9922;	Fax 86-21-6495-7924
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 238 6556;	Fax (65) 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-3-5645-5715;	Fax 81-3-5645-5716
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91 22 696 2790;	Fax 91 22 696 2794
Middle East:	97 14 299 4466	Fax 97 14 299 4664
Thailand:	66 2 651 8733	Fax 66 2 651 8737

If you are looking for further contact information, please visit www.smc.com, www.smc-europe.com or www.smc-asia.com.

SMC®
Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC8612T F 1.0.1.3
Pub.Number: 150200034800A E072003-R01